Symantec™ IT Management Suite powered by Altiris™ technology Migration Guide version 7.0 to 7.5

Symantec™ IT Management Suite powered by Altiris™ technology Migration Guide version 7.0 to 7.5

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing IT Management Suite migration

This chapter includes the following topics:

About IT Management Suite

IT Management Suite (ITMS) combines client and server configuration management with IT asset and service management. It promotes effective service delivery and helps reduce the cost and complexity of managing corporate IT assets. These assets may include desktops, laptops, thin clients, and servers in heterogeneous environments running Windows, Linux, UNIX, or Mac operating systems . You can manage all of the features of the suite through a central console on a common platform: the Symantec Management Platform. This common platform integrates

management functions to accelerate automation for better service, value, and IT efficiency.

IT Management Suite comprises of the following management capabilities:

- Server management
  The server management incorporates a variety of wizards and other features that let you automate configuration, stage tasks, and create policies to manage your servers. The server management capabilities support Windows, UNIX, and Linux operating systems. In addition, the same management disciplines are applied to both physical systems and virtual systems, including both Microsoft Hyper-V and VMware.
- Client management
  The client management helps you discover the resources in your network, and lets you check their state. The reporting tools help you identify problems and take immediate action to fix them. The client management capabilities support Windows, Linux, and Mac operating systems.
- IT asset management
  IT asset management builds upon solid inventory foundations for configuration management. It helps you accurately value both your discoverable and non-discoverable assets, and tracks your assets and your asset-related information. You can manage contracts, software license compliance, and procurement processes as well as the configuration items that are associated with your assets.

About the new features in IT Management Suite 7.5

The architecture of IT Management Suite 7.5 includes several new features and functional enhancements over IT Management Suite 7.0.

The new features are built on the existing technology and therefore improves the manner in which you run the business. The following list highlights few of the main features of IT Management Suite 7.5.

Feature	Description
Symantec Management Console	Gives you a new management interface that consolidates management of common tasks and policies in a single window.

Feature	Description
Cloud-enabled Management (CEM)	Lets you manage endpoints even when the endpoints are not connected to the corporate network through VPN. This functionality helps to improve software and patch deployment coverage of your mobile workforce and telecommuting employees.
Agent registration	Ensures that only trusted Symantec Management Agents (earlier known as Altiris Agents) can communicate with the Notification Server computer.
Legacy Agent Communication (LAC) mode	Enables you to control whether the computers that use older versions of Symantec Management Agent (Altiris Agent) can communicate with the upgraded Notification Server 7.5. Using this option, you can upgrade the agents in your environment in phases rather than updating all of them immediately after you upgrade Notification Server.
Advanced Reporting and Analytics	Gives you the ability to create and view professional reports without the requirement of advanced knowledge of databases or third-party reporting tools. Advanced reporting lets you assess trends using out-of-the-box performance indicators and aggregate data from multiple CMDBs to display a representative view.
Expanded Process Automation Options	Enables you to leverage the power of process automation for making operational, productivity-oriented, and event-based decision rules. Fully empowers the administrator to track the status of a process and create and access documents, wikis, and other information sources.
Smarter Software Lifecycle Management	Lets you tackle the complexity of handling several third-party software applications by creating an easy to use Software Catalog and Software Library. Makes deployment of software easier and faster.

Feature	Description
Robust Patch Management	Assists you to respond to threats by implementing a patch management process. Helps you to assess the effectiveness of a patch management strategy by evaluating key performance indicators.
Improved Inventory Management	Brings together inventory, usage metering, software delivery, and licensing in a streamlined interface so that you can create custom software packages. Includes inventory collection for network devices, file, or registry base-lining and application metering or blacklisting without requiring a separate license.
Centralized Virtual Machine Management	Extends support for VMware and Hyper-V, and automatically discovers your existing virtual machines and maps the relations between them. You can gather virtual machine inventory, such as IP address and disk, memory, CPU utilization and perform tasks such as create virtual machine, modify settings and change power state.
Enhanced Application Virtualization	Includes new administrative tools for advanced customization that you can use to view virtual layer properties, enable or disable layers, and import settings into the software catalog.
Remote Tool Improvements	Includes pcAnywhere Solution that leverages a high performance mirror driver, supports Internet-based remote control (Access Server) and includes multi-monitor support.
Symantec Endpoint Protection Integration	Lets you identify and manage antivirus software from various leading antivirus providers, and initiate virus scans from the Symantec Management Console.
Enhanced Software License Management	Displays a Software License and Software usage Dashboard that you can use to compare the number of licenses you have and the licenses that are in use.

Feature	Description
Redesigned ServiceDesk Solution	Includes all primary ITIL Service Management processes such as, Incident, Problem, Change, and Release Management, and a Knowledge Management system.

For more information, see the “What's new in IT Management Suite 7.5” section in *IT Management Suite 7.5 Planning for Implementation Guide*.

About IT Management Suite migration

IT Management Suite migration involves the transfer of data from your previous computer with IT Management Suite 7.0, to your new computer with IT Management Suite 7.5.

You can perform a migration to IT Management Suite 7.5 in any of the following situations:

- When you want to install the latest available version of IT Management Suite on a new hardware or consolidated hardware.
- When you update the operating system of the computer.
- When you configure a new Configuration Management Database (CMDB).
- When you plan to replace IT Management Suite 7.0 with IT Management Suite 7.5.

Note: For more information about upgrading ITMS 7.1 or later to ITMS 7.5, see the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

See “About the migration methods” on page 16.

About the migration methods

You can plan IT Management Suite migration strategy by understanding the following methods available for migrating the IT Management Suite data:

- Restoring the existing CMDB
  Restore the existing CMDB in the new ITMS installation.
  See “Restoring the Configuration Management Database” on page 35.
- Using the migration wizard

Use the migration wizard to migrate the data that is not present in the CMDB. After you complete the installation of IT Management Suite 7.5, Symantec Installation Manager gives you access to the migration wizard. You can then copy the tool to your previous server and collect the older data. This process works well if you use new hardware to host your new environment. However, if you attempt to reuse previous hardware, then you must use the migration wizard tool before you install IT Management Suite.

See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.

- Copying the data manually
  Copy the data, which the migration wizard cannot migrate, by manual methods.

See "About IT Management Suite migration" on page 16.

See "Preparing for the migration" on page 34.

Important things to know when migrating from Symantec Management Platform 7.0

A migration from Symantec Management Platform 7.0 involves many steps. You should be careful to complete these steps in the recommended order.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About supported IT Management Suite migration paths" on page 18.

In addition to completing the migration steps in the recommended order, you should also pay particular attention to the following items to avoid major problems:

- Database and server backup
  Before you begin the migration, you need to back up the 7.0 Configuration Management Database (CMDB) and the Symantec Management Platform 7.0 server. If you encounter problems during the migration process, you can then revert to these backups. Back up the CMDB to a secure storage location. Making backups before major migration steps can provide more granular recovery from any issues or unplanned outages that might occur during the process.
  See "Backing up the Configuration Management Database" on page 33.
- Product parity
  When you install the 7.5 products, you must install the same products on the 7.5 server that you installed on the 7.0 server. Failure to have product parity can result in the corruption of the database and the operating system when you connect to the 7.0 database. Before you begin the migration, create a list of the 7.0 products that you currently have installed. You can view a list of the installed products on the **Installed Products** page in Symantec Installation Manager.

Symantec recommends that you install any new products after you complete the migration of your 7.0 products.

- SQL collation
  When you restore the CMDB, use the same collation that was used for Symantec Management Platform 7.5. You can restore the database to the same instance of the SQL Server that 7.0 uses, and use a new database name. You can also restore the database to another instance of SQL Server using the previously used database name. You restore the database so that you can connect to it with Symantec Installation Manager during the installation. When you connect to the database, all of its data is migrated.
  See "Restoring the Configuration Management Database" on page 35.
- Server name and IP address
  Symantec recommends that you give the 7.5 server a name and an IP address that is different from the name and IP address of the 7.0 server. You can then run both your old and new server at the same time and reduce functional downtimes.
- Installation path of Symantec Installation Manager
  When you install Symantec Installation Manager on the 7.5 server, you need to use the same installation path that you used on the 7.0 server. If you change the installation path, you cannot upgrade the Symantec Management Agent and the agent plug-ins.
- Mixed mode
  Symantec Management Platform 7.5 does not support mixed mode. A Symantec Management Platform 7.0 server cannot communicate with a Symantec Management Platform 7.5 server.

About supported IT Management Suite migration paths

Symantec supports migrating to IT Management Suite 7.5 if you have one of the following combinations of products:

- Symantec Management Platform 7.0 SP4 and IT Management Suite 7.0 SP2
- Symantec Management Platform 7.0 SP5 and IT Management Suite 7.0 SP2 MR1
- Symantec Management Platform 7.0 SP5 and IT Management Suite 7.0 SP2 MR2
- Symantec Management Platform 7.0 SP5 and IT Management Suite 7.0 SP2 MR3

- Symantec Management Platform 7.0 SP4 and IT Management Suite 7.0 MR1
- Symantec Management Platform 7.0 SP5 and IT Management Suite 7.0 MR2
- Symantec Management Platform 7.0 SP5 and IT Management Suite 7.0 SP2 MR4

See "Migrating from Symantec Management Platform 7.0" on page 28.

About reusing existing hardware to migrate

You can use your existing hardware to migrate to IT Management Suite 7.5 if the hardware supports 64-bit operating system.

If you migrate using the existing hardware that has Notification Server, you must take the following actions:

- Thoroughly test the migration process to ensure that you capture the data properly before re-provisioning.
- Ensure that your business functional needs and requirements are not offline for lengths of time outside of SLAs.
- Develop a reliable agent re-direct process. You must know the new server name before you re-provision Notification Server.

Readiness checklist for IT Management Suite migration

The following tables provide a readiness checklist for IT Management Suite migration before and while you install IT Management Suite:

- Table 1-1 Migration checklist - Before you install IT Management Suite 7.5
- Table 1-2 Migration checklist - While you install IT Management Suite 7.5

Table 1-1 Migration checklist - Before you install IT Management Suite 7.5

Task	Description
Create a backup.	Create a backup of the computer with Symantec Management Platform and the CMDB database.

Table 1-1 Migration checklist - Before you install IT Management Suite 7.5 *(continued)*

Task	Description
Review logs before installing new solutions.	Review the Symantec Management Platform logs for the errors or the warnings. If you find errors or warnings, take note of them and try to resolve them.
Ensure that the computer with IT Management Suite 7.5 has a unique name and IP address.	You must give the computer with IT Management Suite 7.5 a name and an IP address that is different from the name and IP address of the computer with Notification Server 6.x or IT Management Suite 7.0.
Identify the limitations of mixed-mode.	Symantec Management Platform 7.5 does not support mixed mode. A Symantec Management Platform 7.0 server cannot communicate with a Symantec Management Platform 7.5 server.
Copy the product licenses.	Copy the product licenses to a location that is accessible from the computer that has IT Management Suite 7.5.
Recreate Windows server user accounts.	You must recreate the Windows server user accounts on the computer where you install IT Management Suite 7.5.
Use the migration wizard to create a data store file.	You must install the IT Management Suite migration wizard on the computer with IT Management Suite 7.0 and create a data store file. By default, a data store file is created in the `Altiris\Upgrade\Data` directory. Copy the data store file to a location that Symantec Management Platform 7.5 computer can access. You can also create a backup by copying the file to another location. For more information, see the following knowledge base article: http://www.symantec.com/docs/HOWTO9729

Table 1-1 Migration checklist - Before you install IT Management Suite 7.5 *(continued)*

Task	Description
Copy the solutions-specific files.	You must manually copy solution-specific files and settings to a secure location that is accessible from the computer with IT Management suite 7.5.

Table 1-2 Migration checklist - While you install IT Management Suite 7.5

Task	Description
Ensure product parity.	From IT Management Suite version 7.1, a few products replace or absorb other products, or have a new product name. When you install IT Management Suite, you must install at least the same equivalent products that you installed on the computer with Notification Server 6.x or IT Management Suite 7.0.
Use same SQL collation.	When you restore CMDB, use the same collation that was used for Symantec Management Platform 7.0. You can restore the database to the same instance of the SQL Server that Notification Server 7.0 uses, and use a new database name. You can also restore the database to another instance of SQL Server using the previously used database name. You restore the database so that you can connect to it with Symantec Installation Manager during the installation. When you connect to the database, all of its data is migrated.
Use same SIM installation path on 7.0 and 7.5 Symantec Management Platform server.	When you install Symantec Installation Manager 7.5, you need to use the same installation path that you used on the computer with Symantec Installation Manager 7.0. If you change the installation path, you cannot upgrade the Symantec Management Agent and the agent plug-ins.

Table 1-2 Migration checklist - While you install IT Management Suite 7.5 *(continued)*

Task	Description
Import the data from data store file using the migration wizard.	Use the IT Management Suite migration wizard to import the data from the data store file that you created on the previous computer that had IT Management Suite 7.0.

Post-migration checklist for IT Management Suite migration

The following table provides a checklist for the migration tasks you must do after you install IT Management Suite 7.5 and migrate the data:

Table 1-3 Migration checklist - After you install IT Management Suite and migrate your data

Task	Description
Verify the migrated data manually.	You must browse the migrated data such as policies, reports, and packages and verify their state.
Redirect the managed computers.	After you validate the migrated data, redirect the groups of managed computers to report to the new Notification Server 7.5. Once the managed computers report to Notification Server 7.5, use an agent upgrade policy to upgrade their agents.
Recreate hierarchical relationships.	After installing IT Management Suite, if you have used hierarchical relationships and still require them, you must recreate hierarchical relationships and enable replication.

Table 1-3 Migration checklist - After you install IT Management Suite and migrate your data *(continued)*

Task	Description
Configure additional network ports for performing different communication tasks.	Verify and configure the additional network ports for executing specific communication tasks in your environment. Notification Server and endpoints communicate with each other using the standard web ports. By default, the standard web ports, such as port 80 for HTTP communication and port 443 for HTTPS communication, are configured on the computers. Apart from the standard web ports that are configured on computers, you might have to configure additional network ports to perform specific communication tasks. For example, the following tasks require configuration of additional network ports on the computer: ■ Enabling the hierarchy and replication on the Notification Server computer. ■ Downloading packages from Notification Server or package server on the client computer. ■ Downloading the agent for UNIX, Linux, or Mac operating systems from Notification Server on the client computer. The following knowledge base article provides information about all the additional communication tasks and their associated network ports that you can configure in your IT Management Suite 7.5 environment: http://www.symantec.com/docs/DOC6770

Chapter 2

Migrating Symantec Management Platform

This chapter includes the following topics:

About migrating to Symantec Management Platform 7.5

Symantec Management Platform 7.5 requires the Microsoft Windows Server 2008 R2 (64-bit) operating system to host Notification Server. Because Symantec Management Platform 7.0 used a different operating system than Windows Server 2008 R2, you cannot do an automated, on-box upgrade to 7.5.

See "About supported IT Management Suite migration paths" on page 18.

For more information, see topics on system requirements in the IT Management Suite Planning for Implementation Guide.

Note: If you have Symantec Management Platform 7.0 installed on a 64-bit server, you can install the Symantec Management Platform 7.5 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server.

The migration of data from Symantec Management Platform 7.0 to Symantec Management Platform 7.5 requires two steps. In the first step, you connect to a restored instance of the 7.0 Configuration Management Database (CMDB). You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products. Symantec Installation Manager upgrades the existing 7.0 CMDB to the 7.5 schema. This step migrates all of the data in the 7.0 CMDB. In the second step, you use the migration wizard to migrate the data that is not in the CMDB. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings.

See "About data migration when migrating from Symantec Management Platform 7.0" on page 37.

Note: Symantec Management Platform 7.5 does not support a mixed mode of Notification Servers. A 7.0 Notification Server cannot communicate with a 7.5 Notification Server.

The migration process consists of the following phases:

- Prepare
  To minimize downtime and ensure success, use the documentation to create a migration plan for your specific environment. Back up your existing data and create a test environment for evaluating and validating the entire installation and migration process. Symantec recommends that you maintain the test environment for ongoing validation and testing of updates, maintenance packs, and service packs.
- Install and migrate
  During this phase, you install Symantec Management Platform 7.5 on a computer running the Windows 2008 R2 operating system. You also migrate existing Symantec Management Platform 7.0 data from your previous environment to Symantec Management Platform 7.5. You may also manually move some solution-specific data to Symantec Management Platform 7.5.
- Validate
  During the validation phase you confirm that you have set up and configured the new Symantec Management Platform and solutions according to your requirements. The migration wizard verifies the success of the data it imports. However, you should browse to the migrated data such as policies, reports, and packages and verify their state. After you validate the success of the installation and data migration, you redirect groups of managed computers to report to the new 7.5 Notification Server. Once the managed computers report to the 7.5 server, you use an agent upgrade policy to upgrade their agents.

See "Migrating from Symantec Management Platform 7.0" on page 28.

Best practices for migrating to Symantec Management Platform 7.5

Before you begin the migration process, you should develop a migration plan. As you develop your migration plan, you should consider these best practices.

See "About migrating to Symantec Management Platform 7.5" on page 24.

Note: In this guide, the information that applies to version 7.5 of the product also applies to later releases of the product unless specified otherwise.

Table 2-1 Best practices for migrating to Symantec Management Platform 7.5

Best practice	Description
Use a test environment.	Before you install Symantec Management Platform 7.5 in a production environment, create a test environment for evaluating and validating the entire installation and migration process. Symantec recommends that you maintain the test environment for ongoing validation and testing of updates, maintenance packs , and service packs.
Use a pilot test group.	Use a small group of managed computers as a pilot group to test the migration to Symantec Management Platform 7.5. During this pilot test, leave the remaining managed computers supported by the previous version of Notification Server.
Make note of configuration settings before migrating	Make note of the following configuration settings in your current setup before you start the migration process: ■ Task Server settings ■ Agent communication settings ■ Policy refresh settings ■ Membership update settings After you have completed the migration you can then revert to these settings if you want.
Check logs for errors or warnings	Use the Altiris Log Viewer to check the logs for errors or warnings. If you find any errors or warnings, try to resolve them before the upgrade. To open the Log Viewer , in Windows click **Start > All Programs > Symantec > Diagnostics > Altiris Log Viewer**.

Table 2-1 Best practices for migrating to Symantec Management Platform 7.5 *(continued)*

Best practice	Description
Ensure that the Legacy Agent Communication (LAC) mode is enabled.	To allow complete management of legacy agents when the upgrade is in progress, ensure that the **Legacy Agent Communication** mode is enabled. See "About the agent registration after migration from IT Management Suite 7.0" on page 39.
Redirect managed computers in stages.	You can redirect 8,000 computers to a single Notification Server at the same time. After you have successfully redirected a group of computers, upgrade the Symantec Management Agent and agent plug-ins for that group. To upgrade an agent or an agent plug-in, you enable the upgrade policy for the agent or the agent plug-in. **Note:** If you redirect more than 8,000 computers at a time, disable any policies and tasks that communicate frequently with the Symantec Management Agent. For example, disable the inventory, software delivery, and patch policies. Disabling the policies and tasks prevents the console and Notification Server from being very slow. See "About redirecting sites and agents to Notification Server 7.5" on page 41. See "About the Symantec Management Agent upgrade policies" on page 46.
Keep your previous Notification Server.	Maintain your previous Notification Server computers as a record for historical data, policy configuration details, and other settings and data. The following are some examples of when you might remove the old server: ■ After the business functional uses on the old server are matched on the new server. ■ After the data saturation on the new server has the needed depth. ■ When the data in the new Configuration Management Database (CMDB) qualifies against your regulatory standards.
Migrate using a new computer.	You must install the Symantec Management Platform 7.5 products on a computer that is running the Windows Server 2008 R2 operating system. Because this operating system is different from what was required for 7.0, Symantec recommends that you install the 7.5 products on a new computer. **Note:** If you have Symantec Management Platform installed on a 64-bit server, you can install the Symantec Management Platform 7.5 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server.
After the upgrade, disable the **Legacy Agent Communication** mode.	After the upgrade is completed and all agents are upgraded to the latest version, disable the **Legacy Agent Communication** mode. See "About the agent registration after migration from IT Management Suite 7.0" on page 39.

Migrating from Symantec Management Platform 7.0

You must install the Symantec Management Platform 7.5 products on a computer that is running the Windows Server 2008 R2 operating system. Because this operating system is different from what was required for 7.0, Symantec recommends that you install the 7.5 products on a new computer.

For more information, see topics on system requirements in the IT Management Suite Planning for Implementation Guide.

Note: If you have Symantec Management Platform 7.0 installed on a 64-bit server, you can install the Symantec Management Platform 7.5 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server.

The migration of data from Symantec Management Platform 7.0 to Symantec Management Platform 7.5 requires two steps. In the first step, you connect to a restored instance of the 7.0 Configuration Management Database (CMDB). You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products. Symantec Installation Manager upgrades the existing 7.0 CMDB to the 7.5 schema. This step migrates all of the data in the 7.0 CMDB. In the second step, you use the migration wizard to migrate the data that is not in the CMDB. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings.

See "Important things to know when migrating from Symantec Management Platform 7.0" on page 17.

Note: Symantec Management Platform 7.5 does not support a mixed mode of Notification Servers. 7.0 Notification Servers cannot communicate with a 7.5 Notification Server.

Table 2-2 Process for migrating from Symantec Management Platform

Step	Action	Description
Step 1	Back up the 7.0 Configuration Management Database (CMDB) and the Symantec Management Platform 7.0 server.	You must back up the 7.0 CMDB before you begin the migration process. You should also back up the Symantec Management Platform 7.0 server. If you encounter problems during the migration process you can then revert to these backups. Back up the CMDB to a secure storage location. **Warning:** Before proceeding verify that the CMDB and the Symantec Management Platform 7.0 server have been successfully backed up. See "Backing up the Configuration Management Database" on page 33.
Step 2	Prepare for the migration.	On the Symantec Management Platform 7.0 server, complete the precautionary steps before you start the migration process. See "Preparing for the migration" on page 34.
Step 3	Back up the Configuration Management Database (CMDB) again.	Back up the 7.0 database again to capture the most recent data. If you use hierarchy, the backup is also needed to capture the data after the hierarchy is broken. If you break hierarchy, read-only objects are not migrated when you upgrade the database. When you backup the database after you break the hierarchy, these objects are migrated successfully when you connect to the database later in this process. See "Backing up the Configuration Management Database" on page 33.
Step 4	Restore the backed up 7.0 database.	You can use SQL Server Management Studio to restore the database. You can restore the database to the same instance of the SQL Server that 7.0 uses, and use a new database name. You can also restore the database to another instance of SQL Server using the previously used database name. When you restore the database, use the same collation that was used on the Symantec Management Platform 7.0 server. See "Restoring the Configuration Management Database" on page 35. See "Setting the appropriate permissions to the SQL database" on page 36. If you host Microsoft SQL Server on-box, install it on the 7.5 server and copy the backed-up database to the 7.5 server and restore it. If you host Microsoft SQL Server off-box, you can use the same SQL Server or set up a new SQL Server. If you use the same SQL Server, restore the database with a new name to retain the 7.0 database in working order until the migration is successful.

Table 2-2 Process for migrating from Symantec Management Platform *(continued)*

Step	Action	Description
Step 5	Prepare the 7.5 server for the installation.	The 7.5 server must be running the Microsoft Windows 2008 R2 operating system. Symantec recommends that you give the 7.5 server a different name and IP address from the name and IP address of the 7.0 server. Because the Windows server user accounts are not migrated during the migration process, you must recreate them on the 7.5 server. If you use the same user names, they get aligned with the security roles during the migration process. You should also install the following items: ■ SSL and certificates if you use them. ■ Third-party plug-ins that the products you install require. These plug-ins include Microsoft Silverlight 4.0, Adobe Flash Player 10, and Sun Java Runtime 6.
Step 6	Install Symantec Installation Manager on the 7.5 server.	You use Symantec Installation Manager to install the Symantec Management Platform 7.5 products. For more information, see topics on installing Symantec Installation Manager in the IT Management Suite Planning for Implementation Guide. When you install Symantec Installation Manager on the 7.5 server, use the same installation path that you used on the 7.0 server. For example, if the installation path is C:\Program Files on the 7.0 server, then use C:\Program Files on the 7.5 server. If the installation path is D:\Program Files on the 7.0 server, then use D:\Program Files on the 7.5 server. **Warning:** If you change the installation path for Symantec Installation Manager from 7.0 to 7.5, you cannot migrate the Symantec Management Agent and the agent plug-ins.

Table 2-2 Process for migrating from Symantec Management Platform *(continued)*

Step	Action	Description
Step 7	Install the Symantec Management Platform 7.5 products.	You install the Symantec Management Platform 7.5 products with Symantec Installation Manager. When you select the products to install, be sure to install all of the products that are installed on the 7.0 server. Symantec recommends that you install any new products after you complete the migration of your 7.0 products. **Warning:** Failure to install all of the 7.0 products may result in the corruption of the database and the operating system when you connect to the restored 7.0 database. When you install the Symantec Management Platform products, you should also install the migration wizard components. The migration wizard is used in the next step. During the installation process an **Optional Installations** page appears where you have the option to install the migration wizard components. You can also install the migration wizard components at any time with Symantec Installation Manager. At the end of the installation process, Symantec Installation Manager prompts you to apply licenses to the solutions you installed. You can also run Symantec Installation Manager at a later time to apply the licenses. For more information, see topics on installing the Symantec Management Platform products in the IT Management Suite Implementation Guide.
Step 8	Migrate Symantec Management Platform 7.0 data to the 7.5 server with the migration wizard.	You use the migration wizard to migrate 7.0 data that is not in the restored database. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings. See "About data migration" on page 37. See "About data migration when migrating from Symantec Management Platform 7.0" on page 37. To migrate the Symantec Management Platform 7.0 data, follow the steps that are given in a separate process topic: See "Migrating data to Symantec Management Platform 7.5 with the migration wizard" on page 54. **Note:** The migration wizard verifies the success of the data it imports. However, you should browse to the migrated data such as policies, reports, and packages and verify their state. This confirmation should include the data that was in the restored 7.0 database and the 7.0 data that you migrated with the migration wizard.

Table 2-2 Process for migrating from Symantec Management Platform *(continued)*

Step	Action	Description
Step 9	Move solution-specific items from the 7.0 server to the 7.5 server.	Some solution-specific items are not migrated with the CMDB or with the migration wizard. You must manually move these items from the 7.0 server to the 7.5 server. See "About the 7.0 data that you must manually migrate to Symantec Management Platform 7.5" on page 38.
Step 10	(Optional) Define the agent registration policies.	After the upgrade of Symantec Management Agent, the agent sends out registration request to Notification Server to establish the communication. A predefined agent registration policy that is enabled by default allows all computers to register at Notification Server. To restrict access to Notification Server, you can configure custom agent registration policies. See "Creating an agent registration policy" on page 40.
Step 11	Configure and upgrade site servers.	Before you configure your site servers, you should determine how many site servers you need. You must then create the sites and configure the site servers. For recommendations on the number of site servers that you need, see the IT Management Suite Planning for Implementation Guide. Note that a task server computer must have .NET Framework 3.5 feature enabled. See "About redirecting sites and agents to Notification Server 7.5" on page 41. See "Redirecting managed computers to Symantec Management Platform 7.5" on page 43. If you have 7.0 site servers, you must redirect them to the 7.5 Notification Server and upgrade their Symantec Management Agents. The upgrade of the agents also upgrades the site servers. See "About upgrading site servers" on page 45.
Step 12	Verify that sites, subnets, and connection profiles are intact.	You should go to the **Site Server Settings** page, the **Credentials Management** page, and the **Account Management** page to verify that everything has migrated successfully. For more information, see topics on managing sites and subnets and creating connection profiles in the IT Management Suite Planning for Implementation Guide.

Table 2-2 Process for migrating from Symantec Management Platform *(continued)*

Step	Action	Description
Step 13	Download packages to upgraded package servers	If you upgrade the agent on a package server from a 32-bit to a 64-bit, all packages must be downloaded again. See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.
Step 14	Migrate managed computers	From your 7.0 Notification Server, you need to redirect your managed computers so that they report to your new 7.5 Notification Server. You then need to upgrade the Altiris Agent and agent plug-ins on these computers See "About the Symantec Management Agent upgrade policies" on page 46. See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 47.
Step 15	View and manage the agent registration status to verify successful registration.	The **Agent Registration Status** report lets you view and manage all registration requests and completed registrations from Symantec Management Agents. In this report, you can check if the site servers and client computers have successfully established communication with Notification Server. See "Viewing and managing the agent registration status" on page 48.
Step 16	Re-establish hierarchical relationships and enable replication.	If you had hierarchical relationships with Symantec Management Platform 7.0 and still need them, re-establish those relationships in Symantec Management Platform 7.5. Because Symantec Management Platform 7.5 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. Before you re-establish a hierarchical relationship, you must migrate the Notification Servers that are going to be in the hierarchy to Symantec Management Platform 7.5. You can then enable hierarchy replication and peer-based replication. See "Migrating Notification Server computers in a hierarchy" on page 52. For more information, see topics on configuring hierarchy and replication in the IT Management Suite Planning for Implementation Guide.

Backing up the Configuration Management Database

Backing up the Configuration Management Database (CMDB) is the most important fail-safe measure that you can take during the migration process. After you back up the database, you can restore a new instance of the database with the same name or restore the same instance of the database with a new name. You can

connect to the restored database when you install Symantec Management Platform 7.5.You also can use the backup to restore your database to a known good state if anything should happen to compromise your database.

See "Restoring the Configuration Management Database" on page 35.

See "Migrating from Symantec Management Platform 7.0" on page 28.

To back up the Configuration Management Database

1. Open Microsoft SQL Manager Studio.
2. In the left pane, expand the **Databases** folder.
3. In the left pane, under **Databases**, right-click the name of your database.
4. In the right-click menu, click **Tasks > Back Up**.
5. In the **Back up Database** dialog box, in the **Backup type** drop-down list, click **Full**.
6. In the **Backup set** section, enter a name for your backup.
7. In the **Destination** section, add the location where you want your backup file to be stored.

   This location should be a secure storage location, and should not be on the local computer.
8. Click **OK**.

Preparing for the migration

On the Symantec Management Platform 7.0 server, you must complete a number of tasks to prepare for the migration.

See "Migrating from Symantec Management Platform 7.0" on page 28.

To prepare for the migration

1. Verify the completion of all outstanding tasks, policies, package imports, and hierarchy replication schedules.
2. If you use hierarchy, document the hierarchy setup and then remove all hierarchy relationships. The hierarchy setup does not migrate and must be recreated on the 7.5 server. Because Symantec Management Platform 7.5 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy.

   See "Migrating Notification Server computers in a hierarchy" on page 52.
3. Document the Windows Server user accounts you have set up on the 7.0 server. You must recreate these accounts manually on the 7.5 server.

4 Create a backup of your software package files.

5 Create a list of the products that you currently have installed. You must install at least the same products on the 7.5 server that you installed on the 7.0 server. You can install additional products later. You can view a list of the installed products on the **Installed Products** page in Symantec Installation Manager.

Warning: Failure to have exact product parity can result in the corruption of the database and the operating system when you connect to the 7.0 database.

6 Copy your product licenses to a location that is accessible from the 7.5 server. You must reapply the licenses because they do not migrate.

After you migrate the licenses, you must apply them. You can apply the licenses when you install a product or at a later time. You apply the licenses on the **Product Licensing** page in Symantec Installation Manager.

For more information, see the topics about applying the licenses in the IT Management Suite Planning for Implementation Guide.

If your licenses are not downloaded or available, you can download them from the Symantec Licensing Portal. If you cannot apply your old licenses in Symantec Installation Manager, then you must also download new licenses from the licensing portal.

For more information about licenses and using the licensing portal, see the Customer Care Information Center.

Restoring the Configuration Management Database

When you migrate from Symantec Management Platform 7.0, you use a backup copy of the 7.0 database. To migrate the data in the CMDB, you first restore the database. You can restore the database to the same instance of the SQL Server that 7.0 uses, and use a new database name. You can also restore the database to another instance of SQL Server using the previously used database name. If you host SQL Server on-box, you must copy the backed up database to the 7.5 server before you restore it. After you restore the database, you can connect to it when you install the Symantec Management Platform products.

See “Backing up the Configuration Management Database” on page 33.

See “Migrating from Symantec Management Platform 7.0” on page 28.

After you restore the database on a new server, you must also set the appropriate permissions to the SQL database.

See “Setting the appropriate permissions to the SQL database” on page 36.

To restore the Configuration Management Database

1. Open Microsoft SQL Management Studio.
2. In the left pane, on the right-click menu of the **Databases** folder, click **Restore Database**.
3. In the **Restore Database** dialog box, click **From device**.
4. Click the ellipsis option that is associated with the **From device** option that lets you select the database.
5. In the **Specify Backup** dialog box, click **Add**.
6. In the **Locate Backup File** dialog box, select the CMDB that you backed up on the Symantec Management Platform 7.0 server, and click **OK**.
7. In the **Specify Backup** dialog box, click **OK**.
8. In the **Restore Database** dialog box, in **To database**, enter a name for the database, select the database in the **Select the backup sets to restore** section, and click **OK**.
9. After the database is restored, click **OK** in the dialog box that appears.

Setting the appropriate permissions to the SQL database

When you restore the Configuration Management Database (CMDB) on a new server, you must set the appropriate permissions to the SQL database. If you use application permissions to access SQL in Symantec Installation Manager, you must give the application account database ownership (DBO). If you use a specific SQL account to access SQL in Symantec Installation Manager, you must give that account DBO.

See "Restoring the Configuration Management Database" on page 35.

To set the appropriate permissions to the SQL database

1. Open Microsoft SQL Management Studio.
2. In the left pane, under the **Databases** folder, on the right-click menu of the CMDB, click **Properties**.
3. In the **Database Properties** dialog box, in the **Select a page** section, click **Files**.
4. In the right pane of the **Database Properties** dialog box, click the ellipsis option that is associated with the **Owner** option.
5. In the **Select Database Owner** dialog box, click **Browse**.
6. In the **Browse for Objects** dialog box, select the appropriate account and click **OK**.

7 In the **Select Database Owner** dialog box, click **OK**.

8 In the **Database Properties** dialog box, click **OK**.

About data migration

When you migrate to Symantec Management Platform 7.5, you can also migrate the Symantec Management Platform 7.0 data to Symantec Management Platform 7.5.

See "About data migration when migrating from Symantec Management Platform 7.0" on page 37.

Symantec provides the following tools to assist in the process of migrating data to Symantec Management Platform 7.5:

- Symantec Installation Manager
  You use the Symantec Installation Manager to install the migration wizard components. The migration wizard components give you access to the Symantec Notification Server Migration Wizard.
  You also use the Symantec Installation Manager to connect to a restored 7.0 Configuration Management Database (CMDB). When you connect to the 7.0 database, all of its data is migrated.
  See "About installing the Symantec Notification Server Migration Wizard" on page 56.
- Symantec Notification Server Migration Wizard
  You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.5.
  See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.

About data migration when migrating from Symantec Management Platform 7.0

When you migrate from Symantec Management Platform 7.0, you can migrate all of the data in the 7.0 Configuration Management Database (CMDB). Because the 7.0 database is compatible with Symantec Management Platform 7.5, you can connect to a restored instance of the database to migrate the data. Symantec recommends that you use Symantec Installation Manager to connect to the restored 7.0 database.

See "About data migration" on page 37.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "Important things to know when migrating from Symantec Management Platform 7.0" on page 17.

Table 2-3 Symantec Management Platform 7.0 data that is not stored in the database and must be migrated separately

Data	Description
Symantec Management Platform security settings and some general settings	You can migrate these settings with the Symantec Notification Server Migration Wizard. See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.
Windows Server user accounts	You must recreate the user accounts on the new computer.
Some solution-specific files and settings	You must manually move some solution-specific files and settings. See "About the 7.0 data that you must manually migrate to Symantec Management Platform 7.5" on page 38.
Hierarchical relationships	If you used hierarchical relationships and still need them, you must recreate them and enable replication. Because Symantec Management Platform 7.5 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. For more information, see topics on hierarchy in the IT Management Suite Planning for Implementation Guide.
Product licenses	You must copy the product licenses to a location that is accessible from the 7.5 server.

About the 7.0 data that you must manually migrate to Symantec Management Platform 7.5

When you migrate from Symantec Management Platform 7.0 to Symantec Management Platform 7.5, not all of the data is migrated with the migration wizard. You must manually migrate some data from the 7.0 server to the 7.5 server. For some of the migrated data, you must also complete additional manual steps to make the data fully functional.

The following products have some 7.0 data that you must manually migrate to Symantec Management Platform 7.5:

- Inventory Solution
  See "About manual Inventory Solution data migration" on page 70.

- Software Management Solution
  See "About migrating Software Management Solution from 7.0 to 7.5" on page 81.
- Barcode Solution
  See "Migrating to Barcode Solution 7.5" on page 119.
- Real-Time System Management Solution
  See "About manually migrating Real-Time System Manager files and settings" on page 107.
- Real-Time Console Infrastructure Solution
  See "About manually migrating Real-Time Console Infrastructure files and settings" on page 103.

You must also copy the licenses of your Symantec Management Platform 7.0 products to a location that is accessible from the 7.5 server.

About the agent registration after migration from IT Management Suite 7.0

The agent registration feature requires a client computer to be allowed to communicate with Notification Server before this Notification Server can manage the client computer. The agent registration feature works only for the agents that are upgraded to the 7.5 version.

When you upgrade your IT Management Suite from version 7.0 to 7.5, you can pick up the old database. In this case, the **Legacy Agent Communication** (LAC) mode is turned on after the upgrade. If the LAC mode is turned on, the legacy agents can communicate with Notification Server and upgrade.

After Symantec Management Agent is upgraded on your client computers, each upgraded agent sends a registration request to Notification Server to establish communication.

You can check and manage the registration requests in the Symantec Management Console, on the **Agent Registration Status** page, under **Reports > Notification Server Management > Registration**.

In addition to manually managing the registration requests, you can configure agent registration policies that automatically allow or block the requests. By default, an agent registration policy that allows all incoming requests is enabled on Notification Server. During the upgrade process, Symantec recommends that you use only the default agent registration policy. In this case, the client computers that you are currently managing are automatically allowed to communicate with the upgraded Notification Server. After most of the computers have been approved, you can create more restrictive agent registration policies.

You can create an **Agent Registration Policy** in the Symantec Management Console, under **Settings > Agents/Plug-ins > Symantec Management Agent > Settings > Registration Policies**.

After you finish the upgrade process, Symantec recommends turning off LAC mode on Notification Server.

You can manage LAC mode in the Symantec Management Console, on the **Notification Server Settings** page, under **Settings > Notification Server**.

For more information, see the topics about creating an agent registration policy, viewing the Agent Registration Status report, and Legacy Agent Communication in the *IT Management Suite Administration Guide*.

Creating an agent registration policy

Agent registration policies let you automate the agent registration process. An agent registration policy is a set of rules that determine how the incoming registration requests are processed. In the registration request content, Symantec Management Agent sends its host name, MAC address, IP address, FQDN, and logged on user data. The agent registration policy uses the registration request data and the rules that you define within the policy to decide if the request is allowed or blocked.

Warning: The default agent registration policy automatically allows all agents to communicate with Notification Server. You can modify the default policy or create custom policies to restrict the agents that can communicate with Notification Server. If no active policies are available, the status of each incoming registration request is set to pending.

You can view the registration requests in the **Agent Registration Status** report. You can access this report in the Symantec Management Console, under **Reports > Notification Server Management > Registration**.

See "Viewing and managing the agent registration status" on page 48.

To create an agent registration policy

1. In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Agents/Plug-ins > Symantec Management Agent > Settings**.
3. Right-click **Registration Policies**, and then click **New > Registration Policy**.
4. On the right pane, specify the settings of the agent registration policy as follows:

Rules

Lets you define different types of masks for agent identification using the request data. For example, you can define a host name mask, an IP address mask, and a logged on user name mask.

A single policy can contain unlimited number of masks of any type. During the mask matching process, Notification Server treats different mask types as logical AND operation and similar mask types as logical OR operation.

For example, a policy with the following masks allows registration of all agents that have the name that matches mask "*test" and their IP address is either 10.31.12.1, 10.31.12.2, or any from 255 IP addresses from the 10.31.15.0 subnet:

- Host = *test
- IP=10.31.12.1
- IP=10.31.12.2
- IP=10.31.15.0/24

Note: Asterisk is accepted for all rules except for **IP address**. If you want to specify an IP range in a rule, you must define it with the subnet mask. For example, instead of typing **10.31.15.***, you enter **10.31.15.0/24**.

Actions

Lets you define the rule for complied agent processing with the following options:

- **Allow**
  The agents are automatically registered and you do not need to accept them manually.
- **Block**
  Requests from these agents are declined.

Note that if two policies are applicable to a registration request, and one of them allows registration and the other blocks it, the blocking policy is applied to the request.

5 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

6 Click **Save changes**.

About redirecting sites and agents to Notification Server 7.5

Before you redirect sites and agents to the new Notification Server computer, you should develop a redirection plan.

See "Redirecting managed computers to Symantec Management Platform 7.5" on page 43.

Symantec recommends that you keep the Symantec Management Platform 7.0 server and the Symantec Management Platform 7.5 server running at the same time. Over time you incrementally move groups of client computers to the Symantec Management Platform 7.5 server. By maintaining your Symantec Management Platform 7.0 server, you preserve a historical record of your settings and data. You also have more control over what client computers you move and when you move them.

Use the following guidelines when you redirect sites and their site servers to the 7.5 Notification Server:

- When you redirect a site, Symantec recommends that you redirect and upgrade its site server before you redirect any other agents within the site. If there is more than one site server for a location or logical group, migrate the sites servers with their clients in proportional groups. You redirect and upgrade the site servers first so that they are available in the new environment when the agents in the site are redirected.
- After a site server is redirected to the 7.5 Notification Server, you must remove the site server from the 7.0 Notification Server as soon as possible.
  You remove a site server from the 7.0 Notification Server to prevent the agents that are still in the 7.0 environment from communicating with it.
- After you redirect a site server to the 7.5 Notification Server, upgrade the site server immediately.
  To upgrade a site server, upgrade the Symantec Management Agent. You use upgrade policies on the Symantec Management Platform 7.5 server to upgrade the agent.
  See "About upgrading site servers" on page 45.
  See "About the Symantec Management Agent upgrade policies" on page 46.
  See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 47.
- Redirect task servers before you redirect package servers.

How you redirect sites and agents depends on whether you have sites defined and the number of agents in your environment as follows:

No sites are defined.	■ If the number of agents is less than 8,000, any site servers should be redirected to the new Notification Server and then the Symantec Management Agents in the site. ■ If the number of agents is more than 8,000, Symantec recommends that you first define sites in Symantec Management Platform 7.0. Each site should have at least one site server and no site should have more than 8,000 agents. After you define the sites, redirect each site to the new Notification Server. When you redirect a site, redirect the site servers and then the agents within the site.
Sites are defined.	■ If a site has less than 8,000 agents, redirect each site server to the new Notification Server. When you redirect a site, redirect the site servers and then the agents within the site. ■ If a site has more than 8,000 agents, Symantec recommends that you divide the site into smaller sites. ■ If multiple sites share a site server and the sites have a total of less than 8,000 agents, redirect the site servers and sites together. ■ If multiple sites share a site server and the sites have a total of more than 8,000 agents, temporarily remove the site server from the 7.0 system. After you redirect all the sites to the new Notification Server, recreate the shared site server.

Redirecting managed computers to Symantec Management Platform 7.5

The Symantec Management Agents that previously reported to the 7.0 Notification Server need to be redirected to Symantec Management Platform 7.5. When you redirect a group of computers, create a filter for the first group of computers that you want to move. You then target the filter with the targeted agent settings policy and exclude it from the targets of other policies. You can then expand the membership of the filter as needed until it includes all computers.

See “About redirecting sites and agents to Notification Server 7.5” on page 41.

Although 20,000 computers can be managed with a single Notification Server, Symantec recommends that you redirect no more than 8,000 computers at the same time. However, it is possible to redirect up to 15,000 computers to a single Notification Server at the same time.

Note: If you redirect more than 8,000 computers at a time, disable any policies and tasks that communicate frequently with the Symantec Management Agent. Disabling the policies and tasks prevents the console and Notification Server from being very slow.

See "Best practices for migrating to Symantec Management Platform 7.5" on page 26.

For more information, see topics about the **Targeted Agent Settings** page in the *IT Management Suite Administration Guide*.

To redirect computers to Symantec Management Platform 7.5

1. In the 7.5 environment, install a package service and a task service on a site server to handle clients as they are redirected.

   By default, a task service is installed on the Symantec Management Platform server. However, Symantec recommends that you always set up at least one task server to service the client computers.

   Your environment might require multiple site servers. You might elect to redirect a package server and then the clients that use that package server to ensure that packages are available regionally. You can also use virtual machines to serve as temporary site servers during the redirection process. After all the agents for those sites have upgraded, you should then remove the virtual machines.

2. In the 7.0 console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.

3. On the **Targeted Agent Settings** page, select the policy that contains the agents that you want to redirect to 7.5, and click the **Advanced** tab.

4. In the **Alternate URL for accessing NS** section, specify the URL for the 7.5 Notification Server as follows:

   - **Server Name**
     Symantec recommends that you use the fully qualified domain name.
   - **Server Web**
     The Server Web address should be in the following format:
     https://<NS_FQDN>:<port>/Altiris/

5. Click **Save changes**.

About upgrading site servers

You need to upgrade your site servers in a site before you redirect your managed computers in the site to the 7.5 Notification Server. To upgrade a site server, redirect it to the 7.5 Notification Server and upgrade its Symantec Management Agent. Make sure the policies that upgrade the services are enabled to upgrade the site servers. The **Windows Package Server Agent Upgrade** policy upgrades the package servers. The **Task Service Upgrade** policy upgrades the task servers.

See "About redirecting sites and agents to Notification Server 7.5" on page 41.

For a lengthy migration, Symantec recommends that you set up temporary site servers or move your site servers in proportional groups along with their clients. For example, suppose you have 10,000 clients pointing to a Notification Server and four site servers. You do not want to leave either your old or new Notification Server with no site servers. You should either add temporary site servers or move 1/4 of your site servers with 1/4 of your clients.

Symantec recommends you to keep the Legacy Agent Communication mode enabled until all site servers are upgraded.

See "About the agent registration after migration from IT Management Suite 7.0" on page 39.

When you set up package servers, you prepare the network topology for the agent packages that are available from regional package servers. If you have remote sites with a slow connection, you should upgrade their package servers before you upgrade the agents on the clients. By upgrading the package servers, you reduce the load of the package traffic.

Warning: Do not upgrade package servers before their client base is targeted to be upgraded.

If you upgrade the agent on a package server to a 64-bit agent, its 32-bit assemblies are removed and 64-bit assemblies are installed. The existing registry and folder structure for packages remains intact. If you upgrade the agent on a package server to a 32-bit agent, the package server is also upgraded to 32-bit.

After the Symantec Management Agent on a site server is upgraded, the agent sends out registration request to Notification Server to establish the communication. You can view and manage the registration status in the **Agent Registration Status** report.

See "Viewing and managing the agent registration status" on page 48.

After a package server establishes communication with Notification Server, it downloads any new 7.5 system-based packages that the 7.5 Notification Server

hosts. These packages include all solution plug-ins. Any package that has not changed is not re-downloaded.

To access the package server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Package Service > Advanced > Windows > Windows Package Server Agent Upgrade**.

To access the 64-bit task server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Task Service > Advanced > Task Service Upgrade (x64)**.

To access the 32-bit task server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Task Service > Advanced > Task Service Upgrade (x86)**.

About the Symantec Management Agent upgrade policies

You use a Symantec Management Agent upgrade policy to upgrade the 7.0 Symantec Management Agent on your managed computers. To perform the upgrade, you select and enable the appropriate policy and apply it to a set of computers. Upgrade the Symantec Management Agent before you upgrade the agent plug-ins.

See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 47.

The upgrade polices for the Symantec Management Agent are in a **Non Site Server** folder and a **Site Server** folder. To access these folders, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent** and expand the **Windows** folder.

Note: The upgrade policy for the Symantec Management Agent for UNIX/Linux/Mac is in the **UNIX/Linux/Mac** folder.

When you install a 64-bit agent on a computer, 64-bit sub-agents or plug-ins are installed when they are available. If a 64-bit plug-in is not available, a 32-bit plug-in is installed, and it runs in a surrogate service that was created for this scenario. When you install a 32-bit agent on a 64-bit computer, 32-bit sub-agents or plug-ins are installed.

Warning: If you install the 32-bit agent on a 64-bit computer, the agent may have trouble returning some inventory data because it is runs in the WOW64 memory space. Applications that run in the WOW64 memory space do not see the actual registry and file system on a 64-bit computer.

For more information, see topics on file system redirector and registry redirector in the Microsoft MSDN library.

Note: When you install the Symantec Management Agent with a scheduled push install on a 64-bit computer, the 64-bit agent is installed by default. However, if you check the **Force installation of 32-bit Symantec Management Agent on 64-bit systems** option, the 32-bit agent is installed. The option to force a 32-bit installation is on the **Symantec Management Agent Installation Options** dialog box. You access this dialog box when you click the **Settings** option on the **Symantec Management Agent Install** page.

Upgrading the Symantec Management Agent and the agent plug-ins

After you migrate to Symantec Management Platform 7.5, you need to upgrade the Symantec Management Agent and agent plug-ins on the client computers. Upgrade the Symantec Management Agent before you upgrade the agent plug-ins.

See "About the Symantec Management Agent upgrade policies" on page 46.

See "Migrating from Symantec Management Platform 7.0" on page 28.

Warning: If you install the 32-bit agent on a 64-bit computer, the agent may have trouble returning some inventory data because it is runs in the WOW64 memory space. Applications that run in the WOW64 memory space do not see the actual registry and file system on a 64-bit computer.

For more information, see topics on file system redirector and registry redirector in the Microsoft MSDN library.

To upgrade the Symantec Management Agent and the agent plug-ins

1. In Symantec Management Platform 7.5, use filters and targets to create a test group of clients on which to test the upgrade of the agent and the agent plug-ins.
2. For the test group, enable the Symantec Management Agent upgrade policy.
3. For the test group, enable the upgrade policies for the agent plug-ins that correspond to the plug-ins that were installed on client computers before you migrated to 7.5.

4 For the test group, validate that policies, tasks, and other functionality works correctly.

5 For the rest of your client computers, repeat the preceding steps that you performed on the test group.

You can broaden the scope a few thousand clients at a time. Symantec recommends that you do not upgrade more than 8,000 clients at the same time. You can upgrade up to 15,000 clients at the same time. However, you should then disable any policies and tasks that communicate frequently with the Symantec Management Agent.

6 For the clients that are not available during the migration, ask your network team to make the following change:

- Delete the Symantec Management Platform 7.0 DNS A Record.
- Create DNS Alias (CNAME) to direct the host name for Notification Server 7.0 to Symantec Management Platform 7.5.

Keep these settings in place until the upgrade of the agent and the agent plug-ins is completed on all of the remaining clients.

Viewing and managing the agent registration status

The **Agent Registration Status** report lets you view all registration requests and completed registrations from Symantec Management Agents.

In this report, you can see the computers that the **Agent Registration Policy** has automatically allowed or blocked. Note that for direct Symantec Management Agent push installation, the registration is bypassed. However, the computers are still displayed in the report and their status is set to **Allowed**. If no **Agent Registration Policy** applies to the computer, its status is set to **Pending** and the right-click menu lets you manually allow or block it. The right-click menu also lets you revoke the trust of the agents that you have previously allowed.

Note: The agent registration functionality is available only for the Symantec Management Agent 7.5. The legacy agents are managed with the Legacy Agent Communication mode.

See "Creating an agent registration policy" on page 40.

Incoming registration requests are distinguished by the resource keys and they are merged based on the resource keys lookup.

In some situations, duplicate registration requests may appear. For example, if you reinstall the agent on a computer that is already registered on Notification Server, its public key changes. In this case, Symantec recommends that you approve the

registration request to let this computer continue communicating with Notification Server. Also, the duplicate registration requests may appear if you have computers with identical resource keys in your network. In this case, Symantec recommends not to approve the duplicate registration request because it may cause connectivity issues for the resource that previously existed.

If you have duplicate registration requests in your report, the requests are handled as follows:

- If the initial request is allowed and the duplicate request is also allowed, the duplicate request is merged with the existing resource and the report is updated to display a single entry.
- If the initial request is allowed but the duplicate request is blocked, both requests remain in the list. The allowed request represents the actual resource and the duplicate request in blocked or pending state represents the registration attempt from a potentially duplicated resource.

The **Agent Registration Status** report keeps all requests for audit purposes and lets you continuously observe them.

To view and manage the agent registration status

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, expand **Notification Server Management > Registration**, and then click **Agent Registration Status**.

3 (Optional) On the **Agent Registration Status** page, use the right-click menu options to modify the status of the agent. Note that depending on the status of the agent, the right-click options vary.

Allow

You can allow the agents that are in the **Pending**, **Blocked**, or **Revoked** state.

If you allow a blocked agent, the trust is granted next time when the agent sends a registration request to Notification Server.

Block

You can block the agents that are in the **Pending** or **Revoked** state.

If you block a revoked computer, its functional status does not change. However, changing the status lets you differentiate the revoked computers that should never again connect to Notification Server from the revoked computers that may still require your attention.

Note that computers with the **Blocked** status are removed from the list after a predefined period of time if no new registration requests were sent from the same computer during this time. The default period is three months, but you can change it on the **Purging Maintenance** page.

Revoke

You can revoke the registration of the agents that you have previously allowed. For example, you can revoke the registration for the client computer that is reported missing or stolen. After you revoke the agent, it stops receiving policies from Notification Server. Also, a revoked computer cannot be used as a site server.

During the revocation of internal agent trust, the agent encryption key registration gets marked as revoked on Notification Server. Revoked agents do not receive policies and do not run tasks. Also, the revoked agent clears locally stored policies to minimize its activity. After the revocation, Symantec Management Agent is forced to reinitiate the registration process.

The agent receives information about its revoked status next time when it tries to access secured data. Notification Server does not notify the agent about the revocation event when it occurs.

Note that the revoked agent remains in the **Revoked** state even if the agent registration policy allows it. You must manually manage the revoked computers, if you want to change their state.

Migrating Notification Server computers in a hierarchy

The supported method is to migrate the Notification Server computers in the hierarchy from the bottom up. Therefore, you should migrate the lowest child node first and then work up. Ensure that each child Notification Server is migrated to a higher version before its parent.

Because Symantec Management Platform 7.5 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. You might also be able to flatten your hierarchy and reduce the replication traffic and processing on each server including the parent server. Evaluate your topology before you reconnect child servers because they may not be needed.

For more information, see topics on hierarchy in the IT Management Suite Planning for Implementation Guide.

Before you begin the migration process, document your hierarchy settings and the replication rules that you use.

Note: Symantec Management Platform 7.5 does not support a mixed mode of Notification Servers. 7.0 Notification Servers cannot communicate with a 7.5 Notification Server.

You need to ensure that there are no replication jobs currently running at the time that you choose to migrate each Notification Server computer. To check, you can run the **Current Replication Activity** report for the Notification Server computer that you are migrating. The report shows results only if a replication job is currently in progress.

See "Disabling hierarchy replication" on page 53.

When you migrate your Notification Servers that are in a hierarchy, use the procedure that best meets your needs. If you safely fall within the performance and scaling numbers to use a single server, then eliminate your hierarchy. If you need to maintain hierarchy, Symantec recommends migrating all the child servers before the parent server. This method lets you carefully account for the performance on the parent and the child servers as you add servers to the hierarchy and run replication.

Migrating the parent server and eliminating the child servers

1. Remove all hierarchy relationships.
2. Redirect all clients to a single Notification Server.

Migrating the parent server after migrating all of the child servers

1. Remove all hierarchy relationships.
2. Migrate all of the child servers to Symantec Management Platform 7.5.
3. Migrate the parent server to Symantec Management Platform 7.5.
4. Reestablish the hierarchy relationships of the migrated child servers and the migrated parent server along with the replication rules.

Migrating the parent server after migrating half of the child servers

1. Remove the hierarchy from a child server and migrate it to Symantec Management Platform 7.5.

   Do not reconnect the child to the parent at this time.
2. Repeat the first step on a second child server.

   Assuming that you have four Notification Servers, half of your child servers are now in a hierarchy and half of them are not.
3. Remove all hierarchy relationships, and migrate the parent server to Symantec Management Platform 7.5.
4. Immediately, reestablish the hierarchy relationships of the migrated child servers and the migrated parent server along with the replication rules.

   Note: If the parent server is performing upgrades, for example to agents and inventories, the server could be busy. Consequently, the server may be slow during the first replication job.
5. Migrate the two remaining child servers to Symantec Management Platform 7.5.
6. Reestablish the hierarchy relationships of the last two migrated child servers and the migrated parent server along with the replication rules.

Disabling hierarchy replication

Symantec recommends that you disable hierarchy replication on each adjacent hierarchy node. This step prevents any replication data from being sent to a Notification Server computer while it is mid-way through a migration. You need to disable replication on the local server that you are about to migrate. You also must disable replication on any parent and any child Notification Server computers (those that are directly before or after the local server). By completing this step, you prevent the local server from carrying out any of its usual replication jobs.

If you break the hierarchy for the upgrade while you have some replication jobs in the Pending, Retry, or Running state, you should clean them up before performing the upgrade. For more information about cleaning up the replication jobs, see the following knowledge base article TECH141847.

When the Notification Server computer migration has completed, you need to enable hierarchy replication again. Repeat the procedure and select **Enable Replication** from the context menu. Replication resumes as normal.

To disable hierarchy replication on a hierarchy node

1. On the Notification Server computer, open the Symantec Management Console.
2. On the **Settings** menu, click **Notification Server > Hierarchy**.
3. On the **Hierarchy Management** page, on the **Topology** tab, in the diagram view, right-click on the local server node.
4. On the context menu, click **Disable Replication**.

See "Migrating Notification Server computers in a hierarchy" on page 52.

Migrating data to Symantec Management Platform 7.5 with the migration wizard

You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.5.

Note: When you export the settings from IT Management Suite 7.0, all the IT Management Suite 7.0 activities pause till the export is complete. You have to consider this fact if you are exporting the settings from your production server that is interacting with a large number of client computers. The activities on IT Management Suite 7.5 will pause as well while importing the settings from the data file.

See "Migrating from Symantec Management Platform 7.0" on page 28.

Table 2-4 Process for migrating data to Symantec Management Platform 7.5 with the migration wizard

Step	Action	Description
Step 1	Install the migration wizard.	To migrate data with the migration wizard, you must install the migration wizard on your 7.0 server and on the 7.5 server. You use Symantec Installation Manager to install the migration wizard components on the 7.5 server. You then copy the migration wizard installation package to your current Notification Server and install it. See "About installing the Symantec Notification Server Migration Wizard" on page 56. See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.
Step 2	Export 7.0 data to a data store file.	After the migration wizard is installed on the Symantec Management Platform 7.0 server, it starts in export mode. The migration wizard lets you export 7.0 data that is not present in your 7.0 database to a data store file. You can also manually run the migration wizard and export data multiple times. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 3	(Optional) View the data in the data store file.	After you export data to a data store file, you can use Store Browser to view the data that was exported. See "Viewing the data in a data store file" on page 60.
Step 4	(Optional) Compare two data store files.	If you export 7.0 data multiple times, you can use StoreDiff to compare two data store files. StoreDiff creates a data store file that contains the differences between the two data store files. You can then use Store Browser to view these differences. See "Comparing two data store files" on page 61. See "About the Store Browser" on page 63.
Step 5	Copy the migration data to the Symantec Management Platform 7.5 server.	You need to copy the migration data to a location that is accessible to the Symantec Management Platform 7.5 server. By default, a data store file is created in the `Altiris\Upgrade\Data` directory. If package files are exported, this directory also contains a `PackageFiles` folder. You must put the `PackageFiles` in the same directory where you put the data store file. You may also want to copy this data to a neutral location to back up the data.

Table 2-4 Process for migrating data to Symantec Management Platform 7.5 with the migration wizard *(continued)*

Step	Action	Description
Step 6	Import the 7.0 data to Symantec Management Platform 7.5.	On the Symantec Management Platform 7.5 server, use the migration wizard to import the 7.0 data. If the migration wizard is not installed on this computer, you must first install it. See "About installing the Symantec Notification Server Migration Wizard" on page 56. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 63. If you encounter errors when you import data from a data store file, you can export the data that causes errors and then send the subset of the original data store file to Symantec Technical Support so that they can help resolve the problem. See "Exporting data from a data store file" on page 65.

About installing the Symantec Notification Server Migration Wizard

You use the Symantec Notification Server Migration Wizard to migrate data from Symantec Management Platform 7.0 to Symantec Management Platform 7.5. To migrate data with the migration wizard, you must install the migration wizard on your 7.0 server and on the 7.5 server.

See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 57.

See "About data migration" on page 37.

The migration wizard uses exporters to export data and a corresponding set of importers to import data. Each product that has data to migrate has its own set of exporters and importers. By default, the migration wizard exports and imports all of the data. Symantec recommends that you use the default setting to export and import all of the data.

The EXE for the migration wizard is `NSUpgradeWizard.exe`, and it is located in `C:\Program Files\Altiris\Upgrade` by default.

Note: To run the migration wizard, you must be a member of the local administrators group.

Table 2-5 About installing the Symantec Notification Server Migration Wizard

Where you want to install the migration wizard	How to install the migration wizard
Symantec Management Platform 7.5 server computer	Use Symantec Installation Manager on the computer to install the migration wizard components. After you select the products to install, Symantec Installation Manager displays an **Optional Installations** page that includes the **Install Migration Wizard Components** option. If you check this option, the migration wizard components are installed with the selected products. You can also access the **Optional Installations** page at a later time to install the migration wizard components.
Symantec Management Platform 7.0 server computer	Copy the migration wizard installation package from the Symantec Management Platform 7.5 server. The migration wizard installation package has a 32-bit and a 64-bit version. Copy the 32-bit version. You then run the installation package to install the migration wizard. The migration wizard installation package is only available on the 7.5 server if you have installed the optional migration wizard components on that computer. By default, the migration wizard installation package is installed at C:\Program Files\Altiris\Symantec Installation Manager\MigrationPackage. **Note:** The `MigrationPackage` folder contains four files. Two of the files include the word "silent" in their name. Use the migration package files that do not contain the word "silent" to install the migration wizard. **Note:** You can install Symantec Installation Manager on another computer and install only the migration wizard components on that computer. You can then copy the migration wizard installation package to your Symantec Management Platform 7.0 server computer and migrate its data. You might install just the migration wizard if you need to install the Symantec Management Platform 7.5 products on your 7.0 server computer. However, Symantec discourages the reuse of your current server. For more information about installing the Symantec Management Platform 7.5 products on your current server, see HOWTO32427.

About the data that the migration wizard migrates from Symantec Management Platform 7.0

When you migrate from Symantec Management Platform 7.0, you use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data. The migration wizard migrates data that is not in the Configuration Management Database (CMDB). You migrate the data in the 7.0 database when you connect to a restored instance of the 7.0 CMDB. You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products.

See “About data migration” on page 37.

You can migrate the following Symantec Management Platform data with the migration wizard:

- KMS keys
- Credential manager keys
- Selected core settings
- Email settings
- Security roles
- Some event log registry keys

If you store your software packages locally, the migration wizard can also migrate them. When you import the packages, they are imported to the same location they had on the 7.0 server unless you specify an alternate location. The migration wizard can also migrate all patch packages regardless of where they are stored and import them into the default location.

Exporting Symantec Management Platform 7.0 data to a data store file

When you migrate to Symantec Management Platform 7.5, you use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data. When you use the migration wizard, one step in the migration process is to export the 7.0 data to a data store file. By default, the data store file is saved in the `C:\Program Files\Altiris\Upgrade\Data` directory. It has an .adb extension, is easy to copy and back up, and is not dependent on SQL.

See “Migrating data to Symantec Management Platform 7.5 with the migration wizard” on page 54.

See “About data migration” on page 37.

When the migration wizard runs in export mode, it uses exporters to export data. Each product that has data to migrate has its own set of exporters. By default, the migration wizard exports all of the data. Symantec recommends that you use the default setting to export all of the data.

When you export data, additional data migration files may be created and saved in this same directory. For example, when you export locally saved software package files, a `PackageFiles` folder is created that contains folders for all of the package files.

To export Symantec Management Platform 7.0 data to a data store file

1. Install and run the migration wizard on the Symantec Management Platform 7.0 server.

   After the migration wizard is installed on the Symantec Management Platform 7.0 server, it starts in export mode. You can also manually run NSUpgradewizard.exe to start the migration wizard manually. The migration wizard EXE is in the `C:\Program Files\Altiris\Upgrade` directory by default.

   See "About installing the Symantec Notification Server Migration Wizard" on page 56.

2. If the **Welcome** page of the migration wizard appears, click **Next**.

3. On the **Export / Import Task Selection** page, specify a name and location for the data store file, and click **Next.**

   The default name has three parts: the word Store, the date, and the time. The data store extension must be .adb.

4. On the **Password Protection** page, if you want to encrypt the data, enter a password.

   You must then use this password when you import the data on the Symantec Management Platform 7.5 server.

5. On the **Exporter Configuration** page, select the data to export, and click **Next**.

   The options on the **Exporter Configuration** page are as follows:

Products	Lets you select the products whose data you want to migrate. Data is exported only for the products that are checked.
Exporters	Displays the exporters for the product that you select in the **Products** section. Data is exported only for the exporters that are checked in the **Enabled** column.
Filters	Displays a dialog box that lets you filter the data that an exporter migrates as follows: ■ You can uncheck any item that you do not want to migrate. ■ The **Details** option lets you display the **Filter Details** dialog box.

   Symantec recommends selecting all of the available data.

6 On the **Product Readiness Check** page, review the messages, and click **Next**.

This page displays each product that has data that is not included in the export. To view an explanation of why the data is not included, click in the **Message** column.

7 If the product readiness warning message appears, click **Yes**.

This message indicates that not all products meet the product readiness check. To view the explanations for any product readiness warnings, click **No**, and then click **Back**.

8 On the **Task Summary** page, verify that the migration wizard is about to perform the correct tasks, and click **Next**.

9 When the message that the data export has completed successfully appears, click **OK**.

If the data is not exported successfully, a message with instructions appears.

10 (Optional) To display details about each action, check **Show Details**.

11 Click **Finish**.

Viewing the data in a data store file

You use Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.5. When you migrate data with the migration wizard, you export the data to a data store file and then import the data from the data store file. After you create a data store file, you can use the Store Browser to view the data in the data store file.

See "About data migration" on page 37.

See "About the Store Browser" on page 63.

To view the data in a data store file

1 Double-click `StoreBrowser.exe`.

By default, this file is installed at `C:\Program Files\Altiris\Upgrade`.

2 In the **Store Browser**, on the **File** menu, click **Open** and select the data store file.

3 In the **Table Name** column, select a table.

The rows of the table appear in the right pane.

4 To search for specific data in a table, use the following options at the bottom of the right pane:

Starting index	Type a number of a table row, and click **Refresh**. The table row becomes the first row in the right pane.
Find	Type the search criteria, and select the columns of the table in which to perform the search. All rows in the table that match the search criteria are highlighted. To use regular expressions for the search criteria, check **Regex**.
Inverse	Check this option to highlight the text that does not match the search criteria.
Regex	Check this option to perform a search with regular expressions. You then type the regular expression in **Find**.
Refresh	Click this option to complete the search.
Find Next	Click this option to move to the next row that matches the search criteria.

5 If a table row has an **Xml** column, do the following to view the XML:

- Double-click the row.
- In the **Data View for table** dialog box, on the first **Column** drop-down list, click the XML entry.
  The XML appears in the **Value** pane.
- On the second **Column** drop-down list, click **View as XML**.

Comparing two data store files

You can export the same type of 7.0 data to a data store file multiple times. If the data on the 7.0 server changes between exports, then subsequent data store files contain differences. You can use the StoreDiff utility to compare two data store files.

When you compare two data store files that are different, a data store file is created that contains the differences. You then use Store Browser to view this data store file and see the differences. You can use this information to determine the data to import. The data store file that StoreDiff creates cannot be used to import data into Symantec Management Platform 7.5.

See “About the Store Browser” on page 63.

To compare two data store files

1. Start the StoreDiff utility.

   By default, the EXE for the StoreDiff utility is installed in the `C:\Program Files\Altiris\Upgrade` directory. It is installed whenever the migration wizard is installed.

2. On the **Compare Data Stores** dialog box, click **Browse** to select each of the data store files.

3. In **Diff Store**, specify the name and location for the new data store file.

   This data store file highlights the differences between the two data stores.

4. Click **Generate Diff**.

5. On the message that appears, click **OK**.

   The message either states that the two data store files are identical or that a new data store file is generated. If a new data store file is generated, the **Store Browser** opens.

6. In the **Store Browser**, on the **File** menu, click **Open**, and select the new data store file.

7. On the **Diff Store Summary** dialog box, click **OK**.

   This dialog box lists the data store files that are compared in this new data store file.

   This dialog box also has the following color key for the differences between the two data store files:

Green	New data that exists only in the second data store.
Yellow	The deleted data that exists only in the first data store.
Salmon	Data that exists in both data stores but is different.

8. In the left pane of the **Store Browser**, select a table that is shaded with one of the three colors.

   Only the tables that have differences between the two data store files are shaded.

9. In the right pane, view the rows that have differences between the two data store files.

10. If a table row has an **Xml** column, do the following to view the XML:

    - Double-click the row.

- In the **Data View for table** dialog box, on the first **Column** drop-down list, click the XML entry.
  The XML appears in the **Value** pane.
- On the second **Column** drop-down list, click **View as XML**.

About the Store Browser

The Store Browser lets you perform the following tasks:

- Analyze the data before you import it.
  The Store Browser lets you view each table and the data in each row of a table before you import the data. If you perform multiple imports, you can view the data to determine what data to import next.
  See "Viewing the data in a data store file" on page 60.
- Export specific data to create a smaller data store file.
  If you encounter errors when you import data, you may need to send a data store file that contains the data to Symantec Technical Support. The Store Browser lets you export specific data to create a smaller data store file that is more portable.
  See "Exporting data from a data store file" on page 65.
- View differences between two data store files.
  If you have two similar data store files, you can use the StoreDiff utility to create a data store file that highlights their differences. The Store Browser lets you open this data store file and view the differences.
  See "Comparing two data store files" on page 61.

By default, the EXE for the Store Browser is installed at `C:\Program Files\Altiris\Upgrade`. It is installed whenever the migration wizard is installed.

Importing Symantec Management Platform 7.0 data from a data store file

You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data that is not present in your 7.0 database to Symantec Management Platform 7.5. When you use the migration wizard, one step in the migration process is to import the 7.0 data from a data store file.

See "Migrating data to Symantec Management Platform 7.5 with the migration wizard" on page 54.

When the migration wizard runs in import mode, it uses importers to import data. Each product that has data to migrate has its own set of importers. By default, the migration wizard imports all of the data.

You can import all of the data at one time or perform multiple imports and import the data in stages. For example, you can perform an import for each product and then check the data after each import. If you perform multiple imports, you can view the data to determine which data to import next. The data store file organizes all the data except key data by product. The data for each product is stored in tables. The name of each table is *ProductName.TableName*.

If you do not import all of the data initially, you must manually run the migration wizard for subsequent imports. If you import the same data twice, the last import overwrites any previous import.

To import Symantec Management Platform 7.0 data from a data store file

1. Do one of the following to start the migration wizard in the import mode:
   - Install the migration wizard on the Symantec Management Platform 7.5 server with Symantec Installation Manager. By default, the migration wizard starts after it is installed.
     See "About installing the Symantec Notification Server Migration Wizard" on page 56.
   - Run the migration wizard EXE manually.
     When you install the optional migration wizard components, the migration wizard EXE is installed. The EXE for the migration wizard is `NSUpgradeWizard.exe`, and by default it is in the `C:\Program Files\Altiris\Upgrade` directory.
2. If the **Welcome** page appears, click **Next**.
3. On the **Export / Import Task Selection** page, select the data store file you created when you exported the 7.0 data, and click **Next**.
4. On the **Password Protection** page, if a password was used when the data was exported, enter that password.
5. On the **Importer Configuration** page, select the data to import, and click **Next**.

   The options on the **Importer Configuration** page are as follows:

Products	Lets you select the products whose data you want to migrate. Data is imported only for the products that are checked.
Importers	Displays the importers for the product that you select in the **Products** section. Data is imported only for the importers that are checked in the **Enabled** column.

Filters	Displays a dialog box that lets you filter the data that an importer migrates as follows: ■ You can uncheck any item that you do not want to migrate. ■ The **Details** option lets you display the **Filter Details** dialog box. You can sometimes change a value on the **Filter Details** dialog box. For example, when you import a locally stored package file, you can sometimes change the drive to which it is migrated.

6 On the **Product Readiness Check** page, review the messages, and click **Next**.

This page displays each product that has data that is not included in the import. To view an explanation of why the data is not included, click in the **Message** column.

7 On the **Task Summary** page, verify the migration tasks the wizard is about to perform, and click **Next**.

8 When the message that the data import has completed successfully appears, click **OK**.

If the data is not imported successfully, a message with instructions appears.

9 (Optional) To display each action's sub-actions, check **Show Details**.

10 Click **Finish**.

Exporting data from a data store file

If you encounter errors when you import data from a data store file, you may need to send the file to Symantec Technical Support. For a large file, you can use Store Browser to create a data store that is a subset of the original data store file. You can export the data that causes the errors and then send this smaller file to support so that they can help resolve the problem.

See "About the Store Browser" on page 63.

When you export data with the Store Browser, you can select the data tables to export and the specific rows in the data tables. You can specify the rows to export with row numbers, row ranges, or a data string.

To export data from a data store file

1. Double-click `StoreBrowser.exe`.

   By default, this file is installed at `C:\Program Files\Altiris\Upgrade`. It is installed whenever the migration wizard is installed.

2. In the **Store Browser**, on the **File** menu, click **Open**, and select the data store file that contains the data.
3. On the **File** menu, click **Export Data**.
4. In the **Export Data Form** dialog box, in the **Export** column, check the tables whose data you want to export.

   The NSCore.ExporterVersionInfo table is always exported. It contains the data that the migration wizard needs to import the data from the data store file.

5. To export the data for specific rows of a table, click in the **Rows to Export** column and specify the rows as follows:
   - In the **Export Options Form** dialog box, click **Specified Rows**.
   - To specify rows by row number, check **Row Ranges**, and list the rows.
   - To specify the rows that contain a data string, check **Containing String**, and define the string.
   - Click **OK**.
6. In the **Export Data Form** dialog box, in **Destination Store**, specify the name and location for the new data store file.
7. Click **Export**.

Chapter 3

Migrating Inventory Solution

This chapter includes the following topics:

Before you migrate Inventory Solution data

To successfully migrate Inventory Solution data, perform the following preliminary actions:

- Check which items are not migrated with Symantec Notification Server Migration Wizard, and then back up the items.
  See "About Inventory Solution data migration with Symantec Notification Server Migration Wizard" on page 68.
  See "About manual Inventory Solution data migration" on page 70.

About Inventory Solution data migration with Symantec Notification Server Migration Wizard

To successfully migrate Inventory Solution data, you perform the following types of product migration:

- Migration with the Symantec Notification Server Migration Wizard.
  See "Before you migrate Inventory Solution data" on page 67.
  See "Migrating from Symantec Management Platform 7.0" on page 28.
- Manual migration.
  See "About manual Inventory Solution data migration" on page 70.

Note that when you migrate data classes, the old inventory data classes that are migrated are for reporting purposes only. They become obsolete after new inventory policy runs on all systems.

The following solution-specific items are automatically migrated with the Symantec Notification Server Migration Wizard:

- Inventory Solution 7.0 configuration settings are preserved after the upgrade.
- Predefined and custom 7.0 inventory policies and tasks are upgraded to the equivalent 7.5 task-based policies.
- Predefined and custom 7.0 application metering policies.

  Note: 7.0 application metering policies are not migrated if they are located in the application metering folders that have been deprecated in the 7.5 release.

- Predefined and custom 7.0 inventory reports.

  Note: The 7.0 inventory reports that have been deprecated since the 7.1 release are not migrated.

- Predefined and custom 7.0 inventory data classes.
- 7.0 inventory data from 7.0 inventory data classes.
- 7.0 custom inventory script files for Windows and for UNIX, Linux, and Mac. 7.0 custom inventory script files that are included in **Jobs and Tasks**, are treated as 7.0 inventory tasks. Such script files are migrated with the Symantec Notification Server Migration Wizard and do not require any manual migration steps.

- Legacy 6.x custom inventory script files for UNIX, Linux, and Mac created by users on local disk or in shared location.
- Predefined and custom 7.0 application metering reports, data classes, and data.

Note: The 7.0 application metering reports that have been deprecated since the 7.1 release are not migrated.

Note that the new inventory reports pull data from both the legacy data classes migrated from Inventory Solution 6.x, and the new data classes for 7.5. This allows full reporting coverage as systems are upgraded and execute the new Inventory policies.

The following solution-specific items are not migrated with the Symantec Notification Server Migration Wizard because they have been deprecated since the 7.1 release:

Deprecated inventory reports:

- Add/Remove Program Search report
- Count of Distinct Add or Remove Program Applications
- Count of Computers by Office Edition and Version
- Count of Core MS Office Components Installed
- Count of Microsoft Products
- Count of Computers Requiring Resources for Windows XP
- Count of Computers Requiring Resources for Windows Vista
- Windows Vista Upgrade Cost Analysis
- Windows XP Upgrade Cost Analysis
- Count of Products by Version and Manufacturer
- Count of Computers by Product, Version, and Manufacturer

Deprecated application metering reports:

- Application Metering Agent Install Summary
- Application Resource History
- Application Usage
- Application Usage by Computer
- Application by First and Last Start
- Application by Last Stop

Deprecated application metering folders along with all the application metering policies that are located in them:

- Application Monitors
- Application Monitors (Games)
- Application Monitors (MS Office Suite)

The following solution-specific items are not migrated with the Symantec Notification Server Migration Wizard due to extensive changes in the database structure:

- Stand-alone inventory packages.
  See "Manually migrating stand-alone inventory packages " on page 73.
- Legacy 6.x custom inventory script files for Windows created by users on local disk or in shared location.
- Inventory baseline configuration and snapshot files.
  See "Migrating Inventory Solution baseline configuration files" on page 71.

About manual Inventory Solution data migration

When you perform Inventory Solution data migration with the Symantec Notification Server Migration Wizard, some solution-specific files and settings do not migrate. This situation occurs because of the extensive changes in the database structure. To preserve these files and settings, you must manually migrate them from your previous Notification Server computer. After you move these files to your new environment, you must complete configuration steps to make them operate correctly.

See "Before you migrate Inventory Solution data" on page 67.

See the following list for information about manually migrating Inventory Solution items:

- Legacy 6.x custom inventory script files for Windows that are created by users on a local disk or in a shared location.
  You can manually migrate the legacy 6.x custom inventory script files for Windows that you have created in your 7.0 environment. However, you must perform custom configuration steps to make them operate correctly in the new environment.
- Inventory baseline configuration and snapshot files.
  You can also manually migrate your baseline configuration and snapshot files. However, you must perform custom configuration steps to make them operate correctly in the new environment.
  See "Migrating Inventory Solution baseline configuration files" on page 71.
- Stand-alone inventory packages.

You can manually migrate your 7.0 stand-alone packages. However, you should be aware of certain limitations before you choose to do so. To make your 7.0 stand-alone packages operate correctly in the new environment, you must perform custom configuration steps.

Depending on the specific requirements of your organization, it may be preferable to create new 7.5 stand-alone packages.

See "Manually migrating stand-alone inventory packages " on page 73.

Migrating Inventory Solution baseline configuration files

You can also manually migrate your baseline configuration and snapshot files. However, you must perform custom configuration steps to make them operate correctly in the new environment.

Table 3-1 Process for migrating Inventory Solution baseline configuration files with the Symantec Notification Server Migration Wizard

Step	Action	Description
Step 1	Create a backup of your baseline configuration files.	Before you decommission your previous Notification Server computer, back up your baseline configuration files. See "Backing up Inventory Solution baseline configuration files" on page 72.
Step 2	Perform Inventory Solution migration with the Symantec Notification Server Migration Wizard.	Inventory Solution migration with the Symantec Notification Server Migration Wizard lets you automatically migrate a number of Inventory Solution items. See "About Inventory Solution data migration with Symantec Notification Server Migration Wizard" on page 68.
Step 3	Restore your baseline configuration files on the Notification Server 7.5 computer.	After you install the Symantec Management Platform, restore your baseline configuration files on your Notification Server 7.5 computer. See "Restoring Inventory Solution baseline configuration files" on page 72.

Table 3-1 Process for migrating Inventory Solution baseline configuration files with the Symantec Notification Server Migration Wizard *(continued)*

Step	Action	Description
Step 4	Create the **File baseline** task and the **Registry baseline** task.	After you restore your baseline configuration files on your Notification Server 7.5 computer, you need to create the **File Baseline** task and the **Registry Baseline** task to make them function in the new environment. See "Creating the File Baseline task and the Registry Baseline task" on page 73.

Backing up Inventory Solution baseline configuration files

This task is a step in the process for manually migrating your Inventory Solution baseline configuration files.

See "Migrating Inventory Solution baseline configuration files" on page 71.

Before you decommission your previous Notification Server computer, back up your baseline configuration files.

To back up Inventory Solution baseline configuration files

- On your previous Notification Server computer, copy all of your baseline configuration files in the folders **FileBaselinePackage** and **RegBaselinePackage** to a location that you choose.

  By default, your baseline configuration files are located on your previous Notification Server computer in the following location:

  - `%InstallDir%\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management`

  Baseline configuration files may be located in locations other than the default location. Ensure that you also back up the baseline configuration files that you have created outside of the default location.

Restoring Inventory Solution baseline configuration files

This task is a step in the process for manually migrating your Inventory Solution baseline configuration files.

See "Migrating Inventory Solution baseline configuration files" on page 71.

After you install the Symantec Management Platform, restore your baseline configuration files on your Notification Server 7.5 computer.

To restore Inventory Solution baseline configuration files

1. Copy your baseline configuration files and snapshot files from your storage location.
2. On your Notification Server 7.5 computer, paste your baseline configuration and snapshot files to the following default location:

```
C:\Program Files\Altiris\Notification
Server\NSCap\bin\Win32\X86\Inventory\Application Management
```

Creating the File Baseline task and the Registry Baseline task

This task is a step in the process for manually migrating your Inventory Solution baseline configuration files.

See "Migrating Inventory Solution baseline configuration files" on page 71.

After you restore your baseline configuration files on your Notification Server 7.5 computer, you need to create the **File Baseline** task and the **Registry Baseline** task to make them function in the new environment.

To create the File Baseline task

1. In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, right-click **Jobs and Tasks**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, click **File Baseline**.
4. On the **File Baseline** task page, configure the task and click **OK**.

To create the Registry Baseline task

1. In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, right-click **Jobs and Tasks**, and then click **New > Task**.

   In the **Create New Task** dialog box, in the left pane, click **Registry Baseline**.
3. On the **Registry Baseline** task page, configure the task and click **OK**.

Manually migrating stand-alone inventory packages

You can manually migrate your 7.0 stand-alone packages . However, you must perform custom configuration steps to make them operate correctly in the new environment.

Table 3-2 Process for manually migrating stand-alone inventory packages

Step	Action	Description
Step 1	Create a backup of your stand-alone inventory packages .	Before you decommission your previous Notification Server computer, back up your stand-alone inventory packages. See "Backing up stand-alone inventory packages" on page 74.
Step 2	Perform Inventory Solution migration with the Symantec Notification Server Migration Wizard.	Inventory Solution migration with the Symantec Notification Server Migration Wizard lets you automatically migrate a number of Inventory Solution items. See "About Inventory Solution data migration with Symantec Notification Server Migration Wizard" on page 68.
Step 3	Restore your stand-alone inventory packages on your Notification Server 7.5 computer.	After you install the Symantec Management Platform 7.5, restore your stand-alone inventory packages on your Notification Server 7.5 computer. See "Restoring stand-alone inventory packages" on page 75.

Backing up stand-alone inventory packages

This task is a step in the process for manually migrating your stand-alone inventory packages.

See "Manually migrating stand-alone inventory packages " on page 73.

Before you decommission your previous Notification Server computer, back up your stand-alone inventory packages.

To back up your stand-alone inventory packages

- On your previous Notification Server computer, copy all of your stand-alone inventory packages to a location that you choose.

  By default, your stand-alone inventory packages are located on your previous Notification Server computer in the following location:

  ```
  %InstallDir%\Altiris\Notification
  Server\NSCap\Bin\Win32\X86\Inventory\StandalonePackages
  ```

  Stand-alone inventory packages may be located in locations other than the default location. Ensure that you also back up the stand-alone inventory packages that you have created outside of the default location.

Restoring stand-alone inventory packages

This task is a step in the process for manually migrating your stand-alone inventory packages.

See "Manually migrating stand-alone inventory packages " on page 73.

After you install the Symantec Management Platform 7.5, restore your stand-alone inventory packages on your Notification Server 7.5 computer.

To restore your stand-alone inventory packages

1. Copy your stand-alone inventory packages from the location that you chose.
2. On your Notification Server 7.5 computer, paste your stand-alone inventory packages to the following location:

   ```
   C:\Program Files\Altiris\Notification
   Server\NSCap\Bin\Win32\X86\Inventory\StandalonePackages
   ```

About migrating Inventory for Network Devices

You perform the product migration from the version 7.0 according to the migration scenario for Inventory Solution and IT Management Suite.

See "Before you migrate Inventory Solution data" on page 67.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About data migration" on page 37.

Chapter 4

Migrating Patch Management Solution

This chapter includes the following topics:

About migrating Patch Management Solution for Linux data

For Patch Management Solution for Linux, the solution-specific data is migrated when you migrate the product data according to the process that is defined in the "Migrating Symantec Management Platform" chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

After you complete the migration, configure the Novell Mirror Credentials and the Red Hat Network access credentials.

For more information, see the *Patch Management Solution for Linux 7.5 User Guide* at the following URL:

http://www.symantec.com/docs/DOC5772

See “Linux data that is not migrated from 7.0 to 7.5” on page 77.

See “About migrating Linux software update package files” on page 77.

See "SQL tables that are deleted or renamed" on page 80.

Linux data that is not migrated from 7.0 to 7.5

The following table lists the items that are not migrated from 7.0 to 7.5.

Table 4-1 Linux data that is not migrated from 7.0 to 7.5

Item	Description
Patch Management Solution for Linux subscribed channels list	Because of architectural changes, the subscribed channels list is not migrated from 7.0 to 7.5. After you upgrade to 7.5, you must import the software channels list (both Red Hat and Novell) and select the channels for which you want to download updates. You can select the channels on the **Manage > Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Import Patch Data for Novell/Red Hat** page.

About migrating Linux software update package files

In 7.5, the migration wizard lets you export downloaded software update package files from the 7.0 server and store them in the same location as the .adb file. Then, on the 7.5 server, you use the migration wizard to import the files. Make sure that you copy the exported files to the new server or make them available on the network before you run the migration wizard.

The migration wizard imports the exported packages to the location that is specified on the **Core Settings** page. This setting is stored in the CMDB and migrated from the 7.0 server. Do not change this setting on the 7.5 server until you complete the package migration; changing the setting makes packages inaccessible. If the migrated path is not available on the new server, the default location is used. In case of a default installation, the location is: `C:\Program Files\Altiris\Patch Management\Packages\Updates`.

When you run the **Import Patch Data** task, the packages are re-created (but not redownloaded), and then appear in the Symantec Management Console.

Warning: You must install Symantec Management Platform 7.5 at the same location as it was in 7.0. Symantec Management Platform and Migration Wizard do not support migration to a different location.

About migrating Patch Management Solution for Windows data

For Patch Management Solution for Windows, only certain settings can be migrated. Software update policies, bulletins, updates, and software update packages cannot be migrated.

You migrate the product data according to the process that is defined in the "Migrating Symantec Management Platform" chapter. Windows software update package files from Patch Management Solution 7.x version prior to 7.1 SP1 cannot be used by Patch Management Solution 7.5 because of changes to the metadata file used by the solution. Any Windows software update package files that you want to distribute with Patch Management Solution 7.5 must be re-downloaded from the vendor. Therefore, Symantec recommends that in the migration wizard, under **Patch Management Solution for Windows**, you uncheck the **Patch Software Update** filter.

After you migrate to 7.5, you must run the clean-up task that deletes legacy software updates, bulletins, policies, and software update packages. A link to the clean-up task is available on the **Import Patch Data for Windows** page.

If you are using hierarchy, you must run the clean-up task on every Notification Server computer in the hierarchy.

When the clean-up process is complete, verify and validate that the solution settings have been migrated correctly. Then configure the solution and re-create any software update policies that you wish to maintain.

When you re-create the software update policies, associated software update package files need to be re-downloaded from the vendor. The **Legacy Windows Software Update Policies** report lets you view the information about the software update policies that existed in Patch Management Solution 7.x version prior to 7.1 SP1. You can use this report as a reference if you decide to re-create the software update policies using the same bulletins.

For more information on configuring the solution, and downloading and distributing software updates, see the *Patch Management Solution for Windows 7.5 User Guide* at the following URL:

http://www.symantec.com/docs/DOC5768

See “Windows data that is not migrated from Patch Management Solution 7.x version prior to 7.1 SP1 to 7.5” on page 79.

See “About deleting Windows software update package files” on page 79.

See “SQL tables that are deleted or renamed” on page 80.

Windows data that is not migrated from Patch Management Solution 7.x version prior to 7.1 SP1 to 7.5

The following table lists the items that are not migrated from 7.0 to 7.5.

Table 4-2 Windows data that is not migrated from Patch Management Solution 7.x version prior to 7.1 SP1 to 7.5

Item	Description
Software update policies	Software update policies cannot be converted to the new format. You must re-create software update policies manually. The **Legacy Windows Software Update Policies** report lets you view the information about the software update policies that existed in Patch Management Solution 7.x version prior to 7.1 SP1. You can use this report as a reference if you decide to re-create software update policies using the same bulletins. The folders in which software update policies were stored are migrated to 7.5.
Bulletins	Bulletins data is not compatible with 7.5. New information about bulletins is downloaded when you run the **Import Patch Data for Windows** task.
Software updates	Software updates data is not compatible with 7.5. New information about software updates is downloaded when you run the **Import Patch Data for Windows** task.
Software update package files	Patch Management Solution for Windows 7.5 cannot reuse the software update packages from the previous versions. New package files are downloaded from the vendor when you choose to download and distribute software updates.

About deleting Windows software update package files

The 7.5 version of Patch Management Solution for Windows does not support software update packages from versions prior to 7.1 SP1. When you use the migration wizard to import 6.x or 7.x prior to 7.1 SP1 data, software update packages are not imported. When you run the clean-up task, all information about the packages and the packages themselves are deleted.

The clean-up task also deletes the package files that are stored at a UNC location. If you want to keep the package files (for example, for another Notification Server computer to use), Symantec recommends that you configure a new download

location for the 7.5 software update packages on the **Core Services** page before you run the clean-up task.

About migrating Patch Management Solution for Mac data

For Patch Management Solution for Mac, the solution-specific data is migrated when you migrate the product data according to the process that is defined in the "Migrating Symantec Management Platform" chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "SQL tables that are deleted or renamed" on page 80.

SQL tables that are deleted or renamed

When you migrate data from 7.0 Patch Management Solution to 7.5, some of the SQL tables are removed and data is transferred.

The following tables are deleted during the upgrade:

- Inv_Installed_Red_Hat_Software_Update
- Inv_Applicable_Red_Hat_Software_Update
- Inv_Patchable_Red_Hat_Software_Update
- Inv_Installed_Novell _Software_Update
- Inv_Applicable_Novell_Software_Update
- Inv_Patchable_Novell_Software_Update

Table 4-3 shows the data that is moved to the new tables.

Table 4-3 SQL data that is transferred

Table name in 7.0	Table name in 7.5
Inv_Installed_Red_Hat_Software_Update	Inv_InstalledSoftware
Inv_Patchable_Red_Hat_Software_Update	Inv_Patchable_Linux_Software_Update
Inv_Installed_Novell_Software_Update	Inv_InstalledSoftware
Inv_Patchable_Novell_Software_Update	Inv_Patchable_Linux_Software_Update

Chapter 5

Migrating Software Management Solution

This chapter includes the following topics:

About migrating Software Management Solution from 7.0 to 7.5

Most solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

The following are things to consider if you want to migrate Software Management Solution 7.0 to 7.5:

- For 7.5, you do not conduct an actual in-place upgrade. The database is upgraded, however anything on the file system that is not contained in the database needs to be migrated. To migrate, use the migration wizard to put that data into the new structure after 7.5 is installed. This process is called an off-box upgrade.
  Because you perform an off-box upgrade, take the following into consideration:
  - If the software library was located on the Notification Server computer, you must manually move the physical files to the new 7.5 server. The migration wizard does not move these files.
    If you upgrade from a computer with a different IP address or computer name then you need to change the Software Library path manually in the database

and change all the packages to the new location. On the **Software Library Configuration** page, after you change the UNC path and click **Validate** and **Save changes**, the **Managed packages exist** dialog box opens. You must then check **Change existing packages**.

For more information, see the topics about Configuring the Software Library in the *Software Management Solution 7.5 User Guide*.

- If you used a custom local path for the software resources on the 7.0 Notification Server computer, you must recreate the same file structure on the new 7.5 server.

  For example, if the software resources were located on disk F, then disk F must also be on the new 7.5 computer; otherwise, Software Management Solution does not work.

- If a path that is used in a software resource is longer than 248 characters, the physical files cannot be migrated.

  For example, Microsoft SQL Server 2008 folder structure can exceed 248 symbols. You can recreate the folder structure and migrate such files manually.

- The packages on the client computers are not kept and are re-downloaded.
- The Software Portal company logo settings are reset to default after you perform migration from 7.0 SP2 to this version.

Chapter 6

Migrating Deployment Solution

This chapter includes the following topics:

About migration of Deployment Solution

The Altiris™ IT Management Suite 7.5 release contains the Deployment Solution 7.5 version and hence you can migrate Deployment Solution 7.1 that was packaged with ITMS 7.0 to Deployment Solution 7.5.

Before you migrate to Deployment Solution 7.5

Before you start migrating to the latest Deployment Solution, ensure that you create a backup copy of the Task Handler folder and additional Deployment Solution items on a neutral storage location.

Following are the different files of the Task Handler folder and the additional Deployment Solution items are as follows:

Deployment .CAB files	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\Sysprep\Deploy_Cab`
Image packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\image`
PCT packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\PCTPackages`
SOI packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\SOI`
Custom answer files	These files are stored by default at the following location: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Custom`
Copy File packages	These files are stored by default at the following location : `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\CopyFile`
Any drivers that you added to the drivers database	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\DriversDB`

Any drivers that you added for bootwiz	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\bootwiz\Platforms.` Operating system-specific drivers are stored in an applicable operating system folder under the Platforms folder.
Any .PBT files that you added to the NSCap folder	These files are stored by default at the following location: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\PCT`
Any HTTP locations that you created for imaging	You must create a backup of the images in their existing HTTP location. You must recreate the same HTTP location on your new server and move the backup of your images to the new server computer. **Note:** You must take a backup of the HTTP locations only if you migrate to DS 7.5 using a new server computer and connect to the old database. The task is not applicable if you build a new database, or if you upgrade to DS 7.5 using the same server hardware.
Any UNC locations that you created for the Copy File task	You must create a backup of the UNC location and folder structure. You must recreate the same location and folder structure on your new server computer. You must take a backup of the UNC locations only if you migrate to DS 7.5 using a new server computer and connect to the old database. The task is not applicable if you build a new database, or if you upgrade to DS 7.5 using the same server hardware.

To migrate to the latest Deployment Solution

1. Create a backup copy of the Task Handler folder and additional Deployment Solution items on a neutral storage location.
2. Prepare a new computer with Windows Server 2008 R2 x64 as IT Management Suite 7.5.

See “Migrating to Deployment Solution 7.5” on page 86.

Migrating to Deployment Solution 7.5

You can migrate from the Deployment Solution (DS) 7.1 to Deployment Solution 7.5 using any of the following methods:

- Migrate to a DS 7.5 using a new computer
  You can migrate to a new computer and connect to any of the following databases:
  - Connect to an old database
    You can migrate to a new computer and specify to connect to the old database that you had before the migration.
    You must take a backup of the HTTP locations and UNC locations only if you migrate to DS 7.5 using a new computer and connect to the old database. The task is not applicable if you build a new database, or if you upgrade to DS 7.5 using the same server hardware.
    For more information about migrating to DS 7.5 using a new computer and an old database, see To migrate to Deployment Solution 7.5
  - Connect to a new database

  You can migrate to a new computer and build and connect to the new database during the migration. Only Ghost and RapiDeploy imaging tools are supported in Deployment Solution 7.5 for creating and deploying images. Therefore, you can import only the DS 7.1 images, that are created using Ghost and RapiDeploy imaging tools, to DS 7.5 using the resource import tool. The PCT packages, SOI packages, and copy file packages cannot be imported using the resource import tool. In such case, these packages must be newly created on DS 7.5.
  You are not required to take a backup of the HTTP locations and UNC locations if you migrate to DS 7.5 using a new computer and build and connect to a new database.
- Upgrade to DS 7.5 using the same server hardware
  You can replace the DS 7.1 from ITMS 7.1 by DS 7.5 from ITMS 7.5 using the same hardware, server operating system, and database.
  You are not required to take a backup of the HTTP locations and UNC locations if you migrate to DS 7.5 using the same server hardware
  For more information about upgrading to ITMS 7.5, see the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:
  www.symantec.com/docs/doc5697.

The following table provides information about the location of files in Deployment Solution 7.1 and the new location on Deployment Solution 7.5:

Table 6-1

File or package	Location of the item on Deployment Solution 7.1 computer	Location of the item on Deployment Solution 7.5 computer
Deployment .CAB files	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\Sysprep\Deploy_Cab`	`C:\Program Files\Altiris\Notification Server\NSCap\bin\ Deployment\Packages \Sysprep\Deploy_Cab`
Image packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\image`	`C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\Packages\Images`
PCT packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\PCTPackages`	`C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\Packages\PCT`
SOI packages	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\SOI`	`C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\Packages\SOI`
Custom answer files	These files are stored by default at the following location: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32 \X86\Deployment\Custom`	This location is no longer available and used in IT Management Suite 7.5.

Table 6-1 *(continued)*

File or package	Location of the item on Deployment Solution 7.1 computer	Location of the item on Deployment Solution 7.5 computer
Copy File packages	These files are stored by default at the following location : `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\CopyFile`	`C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\Packages\CopyFile`
Any drivers that you added to the drivers database	These files are stored by default at the following location: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\DriversDB`	`C:\Program Files\Altiris\Deployment \DriversDB` `C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\DriversDB`

Any drivers that you added for bootwiz	These files are stored by default at the following location:
	`C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\bootwiz\Platforms.`
	Operating system-specific drivers are stored in an applicable operating system folder under the Platforms folder.
		`C:\Program Files\Altiris\Notification Server\NSCap\bin \Deployment\BDC\bootwiz\ Platforms\WinPE\x64(or x86) \Drivers\CUSTOM\Drivers`
		`C:\Program Files\Altiris\Deployment \BDC\bootwiz\Platforms \WinPE\x64(or x86)\Drivers \CUSTOM\Drivers`
		Note: The operating system-specific drivers are stored in an applicable operating system folder under the **Platforms** folder.

Table 6-1 *(continued)*

File or package	Location of the item on Deployment Solution 7.1 computer	Location of the item on Deployment Solution 7.5 computer
Any .PBT files that you added to the NSCap folder	These files are stored by default at the following location: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32 \X86\Deployment\PCT`	`C:\Program Files\Altiris\Notification Server\NSCap\bin \Win32\X86\Deployment\PCT`
Any HTTP locations that you created for imaging	You must create a backup of the images in their existing HTTP location. **Note:** You must take a backup of the HTTP locations only if you migrate to DS 7.5 using a new computer and connect to the old database. The task is not applicable if you build a new database, or if you upgrade to DS 7.5 using the same server hardware.	You must recreate the same HTTP location on your new computer and move the backup of your images to the new computer.
Any UNC locations that you created for the Copy File task	You must create a backup of the UNC location and folder structure. **Note:** You must take a backup of the UNC locations only if you migrate to DS 7.5 using a new computer and connect to the old database. The task is not applicable if you build a new database, or if you upgrade to DS 7.5 using the same server hardware.	You must recreate the same location and folder structure on your new computer.
Deployment Solution packages on the site server	On the site servers, Deployment Solution packages are stored at `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler`.	On the site servers, Deployment Solution packages are stored at `C:\Program Files\Altiris\Altiris Agent \Package Delivery`.

To migrate to Deployment Solution 7.5

1. Install the latest IT Management Suite on the Windows Server 2008 R2 computer.
2. Copy the files from the neutral storage location to the new structure on the server computer.

   For information on the location of the files
3. Migrate Symantec Management Platform 7.0 data to the 7.5 server with the migration wizard.

   See "Migrating data to Symantec Management Platform 7.5 with the migration wizard" on page 54.
4. In the Symantec Management Console on the **Settings** menu, select **Notification Server > Database Settings**. Select the restored database and click **Save**.
5. Enable the Symantec Management Platform Upgrade policies for site server.

   See "About upgrading site servers" on page 45.

6 Enable the following Deployment Solution upgrade policies:

Ensure that the site server components for Deployment Solution 7.5 are enabled.	After the site servers in your ITMS environment are upgraded, the Deployment site server component is uninstalled and the Task Server component for Deployment Solution 7.5 is upgraded by default You can ensure that the **Deployment Site Server Components – Upgrade** policy is enabled from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration**. Verify that the Deployment site server component is upgraded. To do this step, check the version of Deployment Task Server Handlers in Symantec Management Agent on the site server computer. **Note:** If you want to use an existing site server as a package server and execute Deployment Solution 7.5 tasks on the server, then you must execute the **Deployment Package Server Components – Install** policy on the site server.
Upgrade the deployment plug-ins for Windows, Linux, and Mac.	Enable the Deployment Plug-in upgrade policy for Windows, Linux, and Mac from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration**. Ensure that the Deployment Plug-ins are upgraded by checking the versions of Deployment Solution Plug-in from the Symantec Management Agent.
Upgrade the deployment automation folder for Windows, Linux, and Mac.	Enable the automation folder policy for Windows, Linux, and Mac from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration** .

7 The **Deployment Package Server Components - Install** policy is enabled by default. You can ensure that the policy is enabled from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration**. The **Deployment Package Server** component is deployed on a site server on which the package service is executed.

8 If you have cloned policies in Deployment Solution 7.1 MR1, MR2, and MR3 versions, then you must clone the policies again after the migration is completed. You also have to configure the settings and target collection according to the previous clone policy.

See " Checklist for successful migration from Deployment Solution 7.1" on page 92.

Upgrading Deployment Solution components

The upgrade policy uses filters to determine if an upgrade is necessary. You can access the filters that are used from the **Manage > Filters > Software Filters > Agent and Plug-in Filters** menu.

Checklist for successful migration from Deployment Solution 7.1

After you have completed the process of migrating to the latest Deployment Solution, you can perform the following checks to verify the success of migration.

- Deployment Solution files and folders use the latest version.
- Default Automation packages for Windows x86 and x64 are created. For Linux x86 automation package is created.
- x86 and x64 components, tools, and MSI are available.
- Installation and registry go to the native path and not to WOW Directory or registry for x64 client computers.
- Manually migrated items are copied without any errors.
- After the upgrade of preboot policy, the old preboot images are recreated without any error.
- Installation log and Altiris log contain no error.
- Deployment Solution-specific data that is related to tasks, policies, and settings are preserved when existing database is used.
- All new policies that are related to x64-bit components are present.

- Both x64 and x86 policies point to the correct set of collection.
- All policies are executed successfully and they should install the latest version.
- All new features are available.
- Previously and newly created tasks are available and execute successfully.

Note: In IT Management Suite 7.0, the copy file packages were not listed under the **Symantec Management Console > Settings > Deployment and Migration**. Therefore, after migrating to IT Management Suite 7.5, the copy file packages are not listed under **Symantec Management Console > Settings > All Settings > Deployment and Migration > Copy File Contents**.

Chapter 7

Migrating Monitor Solution

This chapter includes the following topics:

About migrating Monitor Solution

You perform the product migration according to the migration scenario for IT Management Suite. The majority of the solution-specific data is migrated when you migrate according to the process that is defined in the Migrating Symantec Management Platform chapter.

Note: In this guide, the information that applies to version 7.5 of the product also applies to later releases of the product unless specified otherwise.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About data migration" on page 37.

Only the custom or the cloned policies that are enabled before migration remain enabled after you migrate. All default policies are switched off after migration.

After migration the agentless resources are available from the new local Remote Monitor Server (RMS) installed on Symantec Management Platform. The old RMS

is uninstalled during migration. If you want to monitor agentless resources from off-box RMS, you need to install the RMS using the site server settings.

Since Monitor Solution 7.5 supports multiple RMS, you may monitor agentless resources from different locations. As a consequence, you do not need to uninstall an RMS before you install another one.

Agent-based resources are not available after migration. To make agent-based resources available, you need to first upgrade the Symantec Management Agent with the Monitor Plug-in. To upgrade you need to redirect the needed resources to the Symantec Management Platform 7.5 from the old platform. For more information, see topics on Symantec Management Agent in the *IT Management Suite Administration Guide*. You then need to enable the applicable upgrade policy for the Monitor Plug-in.

See "About migrating Monitor Pack for Servers" on page 95.

About migrating Monitor Pack for Servers

When you upgrade the Monitor Pack for Servers component from 7.5, the **Windows 2000** monitor pack is migrated. However, Monitor Pack for Servers 7.5 does not support the **Windows 2000** monitor pack. Note, that the **Windows 2000** monitor pack is not included in a clean installation of Monitor Pack for Servers 7.5.

Any default rule or metric settings are reset to their default values after migration. If you modified a default monitor pack policy to include your custom metrics, the rules and metrics are not migrated. Instead these settings are lost. Only monitor pack cloned policy settings, cloned rule settings, and cloned metric settings are migrated. To work around this issue you can create clones of these policies. Your new custom monitor policies can then be migrated.

Policies that have been updated as part of the 7.5 release are reset unless they were cloned.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 95.

See "About migrating Monitor Solution" on page 94.

Manually cloning your changed default monitor pack policies, metrics, and rules

If you want to migrate changes you have made to a monitor pack default policy, you should clone them. When you migrate a cloned policy, you also need to clone the rules and metrics that you want to migrate. These cloned rules and metrics then

need to be added to the cloned policy. If a cloned policy contains default rules or metrics and you change their settings, the default settings are restored after the migration.

See "About migrating Monitor Pack for Servers" on page 95.

Table 7-1 Process for manually cloning your changed default monitor pack policies, metrics, and rules

Step	Action	Description
Step 1	Clone a changed default policy.	If you want to migrate changes you have made to a monitor pack default policy you should clone them. See "Cloning a changed default policy for migration" on page 96.
Step 2	Clone a changed default rule.	When you migrate a cloned policy, you also need to clone the rules that you want to migrate. See "Cloning a changed default rule for migration" on page 97.
Step 3	Clone a changed default metric.	When you migrate a cloned policy, you also need to clone the metrics that you want to migrate. See "Cloning a changed default metric for migration" on page 97.

Cloning a changed default policy for migration

If you want to migrate changes you have made to a monitor pack default policy, you should clone them.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 95.

To clone a changed default policy for migration

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, click **Monitoring and Alerting > Monitor > Policies > Monitor Policies**.
3. Expand the **Monitor Policies** folders to reach the monitor policy you want to clone.

4 Right-click the policy you want to clone, and click **Clone**.

A clone of the policy is created in the library with **Copy of** prepended to the original name.

5 Select the newly created policy and edit it as needed.

Cloning a changed default rule for migration

When you migrate a cloned policy, you also need to clone the rules that you want to migrate.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 95.

To clone a changed default rule for migration

1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

2 In the left pane, click **Monitoring and Alerting > Monitor > Policies > Rule Library**.

3 In either the **Agent-based** rules table or in the **Agentless** rules table, select the rule to clone.

4 In the toolbar, click the **Clone** symbol.

A clone of the rule is created in the library with **Copy of** prepended to the original name.

5 Select the newly created rule and edit it as needed.

6 Use this cloned rule in a cloned or a new policy to save rule settings after migration.

Cloning a changed default metric for migration

When you migrate a cloned policy, you also need to clone the metrics that you want to migrate.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 95.

To clone a changed default metric for migration

1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

2 In the left pane, click **Monitoring and Alerting > Monitor > Policies > Metric Library**.

3. In either the **Agent-based** rules table or in the **Agentless** metrics table, select the metric to clone.
4. In the toolbar, click the **Clone** symbol.

   A clone of the metric is created in the library with **Copy of** prepended to the original name.
5. Select the newly created metric and edit it as needed.
6. Use this new metric in a cloned rule to save metric settings after migration.

Chapter 8

Migrating Out Of Bound Management Component

This chapter includes the following topics:

Out of Band Management Component no longer supported

The Out of Band Management Component (OOB) is no longer bundled with ITMS. This component was required to define, apply, and maintain the configuration of Intel® Active Management Technology (AMT). Though the OOB Management Component is no longer bundled, existing Real-Time System Manager features continue to function on supported Intel® AMT computers.

When you perform an upgrade from earlier versions of IT Management Suite, the Out of Band Remover utility removes the Out of Band Management Component items from Notification Server and site servers. The Intel® Setup and Configuration Software (SCS) database, commonly referred to as the IntelAMT database remains intact. The Out of Band Remover utility does not affect the Intel® AMT firmware configuration settings on the client computers. If you have already installed a standalone Intel® SCS server it is not affected by the OOBRemover utility.

For more information on how to discover out-of-band capable computers along with guidance migrating your current IntelAMT database to the latest version of Intel® SCS, see http://www.symantec.com/docs/DOC6628.

For Intel AMT support, please use Intel AMT Configuration utilities, that are available for download from Intel.

http://www.intel.com/content/www/us/en/software/setup-configuration-software.html

For BroadCom DASH support, please use Broadcom Advanced Control Suite, that is available for download from BroadCom.

http://www.broadcom.com/support/ethernet_nic/management_applications.php

Symantec Out of Band Remover utility

Out of Band Management Component is removed during the upgrade to ITMS 7.5. An Out of Band Remover utility is installed.

Out of Band Remover utility performs the following:

- Removes all Out of Band items from the Symantec Management Console.
- Removes local Out of Band site servers and Intel SCS service from the local Notification Server.
- Removes Out of Band task plug-ins from all client computers.
- Removes all remote Out of Band site servers.

When the remote Out of Band site servers are removed, the Intel® SCS Service remains on the remote site servers. Intel SCS database is not removed during the uninstall of the Out of Band site servers.

Using legacy data

You can continue using the configuration functionality of the AMT client computers, that Out of Band Management Component provided.

When the local site servers are removed, the database remains in place. To continue using the local site servers, you can download the latest version of SCS Server from Intel, and then install it using the existing database

When the remote site servers are removed, both the database and the remote Intel SCS server remain in place.

To continue using the remote site servers, you need to do the following:

- Download the latest version Intel SCS server and install it using the existing database.
- Download and install the version of Intel SCS Console that corresponds to the version of remote SCS Service that you have installed on the remote site servers.

For more information, visit Intel SCS website.

http://www.intel.com/content/www/us/en/software/setup-configuration-software.html

Chapter 9

Migrating Real-Time Console Infrastructure

This chapter includes the following topics:

About Real-Time Console Infrastructure migration to version 7.5

You can migrate from Real-Time Console Infrastructure 7.0 to Real-Time Console Infrastructure 7.5. In addition to using the migration wizard to migrate, you must complete some manual steps. You need to manually move and store some XML files on the 7.5 computer.

See "Manually migrating Real-Time Console Infrastructure to version 7.5" on page 102.

Manually migrating Real-Time Console Infrastructure to version 7.5

You can use the Symantec Notification Server Migration Wizard to help you migrate Real-Time Console Infrastructure to version 7.5.

Table 9-1 Process for manually migrating Real-Time Console Infrastructure 7.0 to version 7.5

Step	Action	Description
Step 1	Export data from the previous Notification Server computer.	Use the Symantec Notification Server Migration Wizard to migrate the items that are not stored in the SQL database. When you use the migration wizard, you must export Notification Server data to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 2	Import the exported data from the previous Notification Server computer to the Symantec Management Platform 7.5.	You use the Symantec Notification Server Migration Wizard to migrate the previous Notification Server data to Symantec Management Platform 7.5. When you use the migration wizard, you must import the old data from a data store file. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 63.
Step 3	Move and store Real-Time Console Infrastructure files and settings.	You need to move and store some XML files from the old Notification Server computer to the Symantec Management Platform 7.5 computer. See "About manually migrating Real-Time Console Infrastructure files and settings" on page 103.

About manually migrating Real-Time Console Infrastructure files and settings

The majority of your Real-Time Console Infrastructure Solution data is migrated when you migrate your Real-Time Console Infrastructure to your new 7.5 Symantec Management Platform. However, you must manually migrate some files. To migrate these files, you use your previous Notification Server computer files and move them to your new 7.5 Symantec Management Platform environment.

Table 9-2 Real-Time Console Infrastructure files path

Old Notification Server path	Symantec Management Platform 7.5 path
`C:\Program Files\Altiris\RTCI\Web\UIData\EventFilter_AMT.xml`	Same location on the new 7.5 Symantec Management Platform.
`C:\Program Files\Altiris\RTCI\Web\UIData\EventFilter_DASH.xml`	Same location on the new 7.5 Symantec Management Platform.

Table 9-2 Real-Time Console Infrastructure files path *(continued)*

Old Notification Server path	Symantec Management Platform 7.5 path
`C:\Program Files\Altiris\RTCI\Web\UIData\PortCheck.xml`	Same location on the new 7.5 Symantec Management Platform.

How to validate Real-Time Console Infrastructure after the migration

You need to check if your previous settings and options have been correctly migrated. In addition, if you had any scheduled tasks on your old Notification Server computer, check that those predefined tasks have been correctly migrated.

Predefined tasks may consist of the predefined time schedule, computer profiles, connection profiles, and credential profiles as follows:

- Connection and credential profiles
  If you have used a security certificate in your connection settings, you need to make sure that it has a correct server name and location.

  Note: Credentials must be updated in the connection profile, since runtime credentials are no longer available, once the Out of Band Management Component is removed, during the IT Management Suite 7.5 installation.

  For more information, see the topics about connection profiles in the *IT Management Suite 7.5 Administration Guide*.
- Get out-of-band inventory
  For more information, see the topics about collecting and viewing Intel AMT and DASH inventory in the *Real-Time System Management 7.5 User Guide*.
- Power management
  For more information, see the topics about managing the power state of computers remotely in the *Real-Time System Management 7.5 User Guide*.
- Update Intel AMT credentials
  For more information, see the topics about updating Intel AMT credentials in the *Real-Time System Management 7.5 User Guide*.
- Update Intel AMT settings
  For more information, see the topics about updating Intel AMT settings and configuring Intel AMT in the *Real-Time System Management 7.5 User Guide*.
- Update out-of-band alert settings

You need to make sure that you have a correct **SNMP server** for Intel AMT and ASF and the correct **Destination URL** for DASH.

For more information, see the topics about updating Intel AMT and DASH alert settings in the *Real-Time System Management 7.5 User Guide*.

Chapter 10

Migrating Real-Time System Manager Solution

This chapter includes the following topics:

About Real-Time System Manager migration to version 7.5

You can migrate from Real-Time System Manager 7.0 to Real-Time System Manager 7.5. In addition to using the migration wizard to migrate, you must complete some manual steps. You need to manually move and store some XML files on the 7.5 computer.

See "Manually migrating Real-Time System Manager to version 7.5" on page 106.

Manually migrating Real-Time System Manager to version 7.5

You can use the Symantec Notification Server Wizard to help you migrate Real-Time System Manager to version 7.5.

Table 10-1 Process for manually migrating Real-Time System Manager 7.0 to version 7.5

Step	Action	Description
Step 1	Export the data from the previous Notification Server computer.	Use the Symantec Notification Server Migration Wizard to migrate the items that are not stored in the SQL database. When you use the migration wizard, you must export Notification Server data to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 2	Import the exported data from the previous Notification Server computer to the Symantec Management Platform 7.5.	You use the Symantec Notification Server Migration Wizard to migrate the previous Notification Server data to Symantec Management Platform 7.5. When you use the migration wizard, you must import the data from a data store file. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 63.
Step 3	Move and store Real-Time System Manager files and settings.	You need to move and store some XML files from the old Notification Server computer to the Symantec Management Platform 7.5 computer. See "About manually migrating Real-Time System Manager files and settings" on page 107.

About manually migrating Real-Time System Manager files and settings

The Real-Time System Manager Migration Wizard contains the following exporter and importer objects:

- Boot Redirection task
- Network Filtering task
- Password Management task
- Process Management task
- Service Management task

The majority of your Real-Time System Manager data is migrated using the migration wizard. However, to have full predefined functionality, you must move some files. You need to manually move and store these files from the old Notification Server computer to the new 7.5 computer.

By default, the files that need to be moved are located on your previous Notification Server in specific locations.

Table 10-2 Real-Time System Manager files path

Notification Server path	Symantec Management Platform 7.5 path
`C:\Program Files\Altiris\RTSM\Web\Bin\WebTerminal.config`	Same location on the new 7.5 Symantec Management Platform.
`C:\Program Files\Altiris\RTSM\Web\UIData\PingFilter.xml`	Same location on the new 7.5 Symantec Management Platform.
`C:\Program Files\Altiris\RTSM\Web\UIData\CBFilters.xml`	Same location on the new 7.5 Symantec Management Platform.

How to validate Real-Time System Manager after the migration

After you finish the migration process, it is necessary to validate the migrated items. In fact, you need to make sure that these items have been correctly migrated to your new 7.5 Symantec Management Platform environment. They still should have the same predefined functionality. You need to check the following items:

- Connection settings and credential profiles
  If you have used a security certificate in your connection settings, you need to make sure that it has a correct server name and location.

  Note: During installation of ITMS 7.5 Out of band Management Component is removed. Runtime credentials are no longer available. You need to update connection profiles, adding current credentials.

  For more information, see the topics about connection profiles in the *IT Management Suite 7.5 Administration Guide*.
- Boot Redirection
  You need to manually move and store your redirection images from your old Notification Server to your new 7.5 Symantec Management Platform environment. For more information, see the topics about booting multiple computers from another device in the *Real-Time System Management 7.5 User Guide*.
- Network Filtering

You need to manually move and store your predefined custom network filters from your old Notification Server to your new 7.5 Symantec Management Platform environment.

For more information, see the topics about filtering network traffic on multiple computers in the *Real-Time System Management 7.5 User Guide*.

- Password Management

  For more information, see the topics about resetting a local user password on multiple computers in the *Real-Time System Management 7.5 User Guide*.

- Process Management

  For more information, see the topics about running or stopping a process on multiple computers in the *Real-Time System Management 7.5 User Guide*.

- Service Management

  For more information, see the topics about running or stopping a service on multiple computers in the *Real-Time System Management 7.5 User Guide*.

Chapter 11

Migrating pcAnywhere Solution

This chapter includes the following topics:

Before you begin the migration from pcAnywhere Solution 7.0

The newer Symantec Management Agent and pcAnywhere agents replace the older Altiris Agent and the Carbon Copy Agent.

Note: In this guide, the information that applies to current version of the product also applies to later releases of the product unless specified otherwise.

Before you begin the migration from 7.0, ensure that the following tasks are completed:

- Back up your current 7.0 server and databases before you start any migration work.
- Verify and complete all outstanding tasks, policies, package copies, and hierarchy replication schedules, if they are in use.
- Disable all hierarchy and peer-based replication schedules, if they are in use.
- Review the data available in the pcAnywhere reports and verify if the data is correctly displayed.
- Back up the current database to capture the most recent one.

- Shut down the 7.0 Notification Server computer.

See "Migrating from pcAnywhere Solution 7.0" on page 111.

Migrating from pcAnywhere Solution 7.0

Ensure that you have performed the required steps to migrate to the IT Management Suite.

See "Before you begin the migration from pcAnywhere Solution 7.0" on page 110.

Note: In this guide, the information that applies to version 7.0 of the product also applies to later releases of the product unless specified otherwise.

To migrate from 7.0 with pcAnywhere Solution

1. Prepare the target server for the installation of IT Management Suite 7.5.

   For information on Symantec IT Management Suite platform support, seehttp://www.symantec.com/docs/HOWTO9965.

2. Install IT Management Suite or pcAnywhere Solution onto the target server (with migration components within the optional components).
3. Use the migration wizard to export 7.x data from the source server.
4. Copy the x86 migration package from your IT Management Suite 7.5 server to the IT Management Suite 7.0 server.

   The package is located at `Program Files\Symantec Installation Manager \Migration Package\`

   Multiple migration packages are launched and installed for pcAnywhere Solution.

5. From the IT Management Suite 7.0 server, run the migration package that was copied from the ITMS 7.5 server.

   From the `program files\ upgrade` directory on the 7.0 server, run the migration wizard (`NSUpgradeWizard.exe`).

   The migration wizard exports KMS and CM keys into a data store file (*.adb).

6. Create a data store file (`*.adb`).
7. Run the x64 migration wizard on IT Management Suite 7.5 server and import the backed up `.adb` file.

8 Redirect package servers first to prepare the topology for regionally available agent packages.

Alternatively, package servers can be temporarily added to the topology during the migration process and removed after 7.0 package servers have completed their upgrades.

9 Redirect all the agents that earlier reported to the 7.0 server to the new server.

You can use Notification Server 7.0 agent settings to redirect.

10 Enable upgrade policies for the Symantec Management Agent and the pcAnywhere Solution plug-ins.

Re-establish hierarchy relationships.

Re-enable hierarchy and peer-based replication.

See "About the Symantec Management Agent upgrade policies" on page 46.

Chapter 12

Migrating CMDB Solution

This chapter includes the following topics:

About migrating CMDB Solution

You perform the product migration from 7.0 according to the migration scenario for Asset Management Solution and IT Management Suite.

Note that the license check for CMDB Solution has been removed making CMDB Solution available to all Altiris solutions as a feature. You can now install CMDB Solution as a feature of Inventory, Client Management Suite, and Server Management Suite. It is already installed with Asset Management Suite, ServiceDesk, and IT Management Suite. Note that in a hierarchy, CMDB Solution must be installed on the parent Notification Server. Do not install CMDB Solution on a child Notification Server.

See “About migrating Asset Management Solution” on page 114.

See “Migrating from Symantec Management Platform 7.0” on page 28.

See “About data migration” on page 37.

Chapter 13

Migrating Asset Management Solution

This chapter includes the following topics:

About migrating Asset Management Solution

You perform the product migration from Asset Management Solution 7.0 according to the migration scenario for IT Management Suite. No manual solution-specific migration steps are required. The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About data migration" on page 37.

Chapter 14

Migrating Barcode Solution

This chapter includes the following topics:

About migrating Barcode Solution

You can migrate from Barcode Solution 7.0 to Barcode Solution 7.5.

The majority of the Barcode Solution data is migrated when you migrate the Configuration Management Database (CMDB) using the migration wizard. In addition to using the migration wizard to migrate, you must execute some manual steps. The synchronization profile settings are not automatically upgraded, but can be manually exported to XML files before migration, then imported to the new server.

See "Migrating to Barcode Solution 7.5" on page 119.

Before you migrate to Barcode Solution 7.5

Before you start migrating to Barcode Solution 7.5, ensure that the following tasks are completed:

Table 14-1 Prerequisites for migrating to Barcode Solution 7.5

Step	Action	Description
Step 1	Upload and synchronize the data from handheld devices to the previous Notification Server computer.	You must finish uploading and synchronizing all your data from the handheld device to the previous version of Barcode Solution before you migrate. Failure to synchronize the data means you might lose existing data. You cannot upload the data from the old version of Barcoder to the new version of Barcode Solution. Therefore, you must first upload existing data to the previous version of Barcode Solution, and then migrate the data to Barcode Solution 7.5. See "Synchronizing data from handheld devices to Notification Server" on page 117.
Step 2	Ensure that all batches in the upload verification section have been processed.	You must verify your asset data before you load it into the Configuration Management Database. You verify asset data using the **Batch Uploads** page from the Symantec Management Console of Notification Server of previous version. If you migrate from IT Management Suite 7.0, then any unprocessed batches will be available to process in 7.5. However, Symantec recommends that you still undertake this step as a best practice. See "Verifying asset data before loading it into CMDB" on page 118.

Table 14-1 Prerequisites for migrating to Barcode Solution 7.5 *(continued)*

Step	Action	Description
Step 3	Back up the Barcode Solution default synchronization profile.	Use the Symantec Management Console of previous version's Notification Server computer to export your default synchronization profile. To manually migrate the default synchronization profile settings, you must use the Symantec Management Console to export the settings to an XML file. Store the XML file on a neutral storage location. See "Backing up the Barcode Solution default synchronization profile" on page 118.

Synchronizing data from handheld devices to Notification Server

You must finish uploading and synchronizing all your data from the handheld device to the previous version of Barcode Solution before you migrate. Failure to synchronize the data means you might lose existing data. You cannot upload the data from the old version of Barcoder to the new version of Barcode Solution. Therefore, you must first upload existing data to the previous version of Barcode Solution, and then migrate the data to Barcode Solution 7.5.

Any data that is specified in the **Synchronization Profiles** page is uploaded to the Barcode device in the initial synchronization. It may involve the transfer of a significant amount of data. Ensure that there exists a good connection from the handheld device, either through a wireless or a synchronization cradle, with Notification Server 7.0 computer.

See "Migrating to Barcode Solution 7.5" on page 119.

To synchronize data from handheld devices to the previous version of Notification Server

1. Ensure that the Barcode device has a connection to the previous Notification Server computer, either through a wireless or a synchronization cradle.
2. On the Barcode device, click **Start > Programs > Symantec Altiris Barcoder**.
3. Select **Synchronize** from the menu option.

4 Enter your security credentials and click **Login**.

Your password and user name are cached for an hour on the handheld device. If you do not use it for over an hour, you must reenter your security credentials. Closing the application clears the cached credentials; they need to be reentered on launching the application again.

5 Select the synchronization profile to use, and click **Next**.

6 Choose one of the synchronization options, and click **Sync**.

Verifying asset data before loading it into CMDB

You must verify the asset data before you load the data into the Configuration Management Database. You verify the asset data from the **Batch Uploads** page.

See "Migrating to Barcode Solution 7.5" on page 119.

To verify asset data before you load the data into the Configuration Management Database

1 In the Symantec Management Console of Notification Server 7.0, on the **Home** menu, click **Service and Asset Management > Barcode**.

2 In the left pane, click **Barcode Solution > Manage Changes > Batch Uploads**.

3 In the **Batch uploads** page, select the batch of uploaded data that you want to verify.

4 Click **View Batch Details** select a resource and click **Resource Details** to view its changed details.

5 In the **Batch Details** dialog box, select a resource and click **View Resource Details** to view its changed details.

6 Select a resource from the list in the top section and click **Accept** to return to the **Batch Details** dialog box.

7 In the **Batch Details** dialog box, click **Accept Batch** to save your changes to the database.

Backing up the Barcode Solution default synchronization profile

Before you decommission your previous Notification Server computer, back up your Barcode Solution default synchronization profile. To manually migrate the default synchronization profile settings, you must use the Symantec Management Console to export the settings to an XML file. Store the XML file to a neutral storage location.

Name the clone default profile `Default profile 7.0` or similar. The default profile already exists on IT Management Suite 7.5. Therefore, renaming the cloned default profile ensures that the profile can be identified differently in the IT Management

Suite 7.5 environment. By being uniquely identifiable, the cloned default profile is not overwritten.

This task is part of the process for manually migrating your Barcode Solution files settings. After you complete this task, you can complete the rest of the process.

See "Migrating to Barcode Solution 7.5" on page 119.

To back up the Barcode Solution default synchronization profile

1. On Notification Server 7.0 computer, in the Symantec Management Console, on the **Home** menu, click **Service and Asset Management > Barcode**.
2. In the left pane, expand **Barcode Solution > Synchronization Profiles > Default**.
3. Right-click **Default**, and click **Export**.
4. Save the `Default.xml` file to a neutral storage location.
5. Clone the default profile to ensure that it can be identified in the IT Management Suite 7.5 environment.

Migrating to Barcode Solution 7.5

The majority of the Barcode Solution data is migrated when you migrate your Configuration Management Database (CMDB) using the migration wizard. However, you must manually migrate your default synchronization profile settings. To migrate these settings you use the console to export them into an XML file. You then import this XML file after you install your new Symantec Management Platform. In addition, Symantec recommends that you finish synchronizing all your data from the handheld devices. Also, ensure that you verify your asset data before you load it into the CMDB by processing all batches.

See "About migrating Barcode Solution" on page 115.

Table 14-2 Process for migrating to Barcode Solution 7.5

Step	Action	Description
Step 1	Prepare to migrate.	Before you migrate to Barcode Solution 7.5, you must execute some manual steps to prepare the environment of the previous Barcode Solution for the migration. See "Before you migrate to Barcode Solution 7.5" on page 115.

Table 14-2 Process for migrating to Barcode Solution 7.5 *(continued)*

Step	Action	Description
Step 2	Perform the migration.	Use the Symantec Notification Server Migration Wizard to export and import your data. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 63. **Warning:** Because Barcode Solution relies on CMDB Solution, the CMDB data must be imported at the same time or before you import the Barcode data. For this reason, ensure that you have **CMDB Solution** selected in the **Exporter Configuration** page of the Symantec Notification Server Migration Wizard.
Step 3	Perform post-migration tasks.	After executing the migration wizard, you must restore the Barcode Solution default synchronization profile file. Use the Symantec Management Console of Notification Server 7.5 to import your default synchronization profile settings from an XML file. See "Performing post-migration tasks" on page 120.

Performing post-migration tasks

After you install Symantec Management Platform 7.5 and have run the migration wizard, you can import and restore the default synchronization profile XML file of previous version's Barcode Solution to Barcode Solution 7.5

See "Migrating to Barcode Solution 7.5" on page 119.

To import and restore the default synchronization profile of previous version's Barcode Solution to Barcode Solution 7.5

1. On your new Notification Server computer, in the **Symantec Management Console**, go to **Home > Service and Asset Management > Barcode**.
2. In the left pane, expand **Barcode Solution > Synchronization Profiles > Default**.
3. Right-click the **Synchronization Profiles** folder, and click **Import**.
4. Browse to the default synchronization profile XML file of previous version's Barcode Solution.
5. Click **Open** to import the XML file.

Chapter 15

Migrating Workflow Solution

This chapter includes the following topics:

About migrating Symantec Workflow

You perform the Symantec Workflow data migration from 7.0 according to the migration scenario for IT Management Suite.

See “Migrating from Symantec Management Platform 7.0” on page 28.

See “About data migration” on page 37.

After you migrate your data, you must upgrade your Workflow processes. For information about upgrading your Workflow processes, see the topic "Process for upgrading Workflow" in the *Symantec™ Workflow 7.5 User Guide* at http://www.symatnec.com/doc/DOC5941.

Chapter 16

Migrating Inventory Pack for Servers Solution

This chapter includes the following topics:

About migrating Inventory Pack for Servers

You perform the product migration from the version 7.0 according to the migration scenario for Inventory Solution and IT Management Suite.

See "Before you migrate Inventory Solution data" on page 67.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About data migration" on page 37.

Chapter 17

Migrating ServiceDesk Solution

This chapter includes the following topics:

About migrating from ServiceDesk 7.0

Because the ServiceDesk installation overwrites all existing workflow processes, an in-place same-server upgrade is not currently supported (it can potentially affect custom configurations).

For more information, see Symantec™ ServiceDesk 7.5 MP1 Implementation Guide.

You can leverage some data from ServiceDesk 7.0 MR2 in ServiceDesk 7.5.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets
- Close Problem Management tickets

- Closed knowledge base submission tickets
- End-User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP2, and 7.1 SP2 tickets to ServiceDesk 7.5

Chapter 18

Migrating Virtual Machine Management Solution

This chapter includes the following topics:

Migrating from Virtual Machine Management 7.0

There are no manual solution-specific migration steps to perform. The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

Note: In this guide, the information that applies to version 7.5 of the product also applies to later releases of the product unless specified otherwise.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "About data migration" on page 37.

Chapter 19

Migrating Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

About migrating Symantec Endpoint Protection Integration Component

The latest version of Symantec Endpoint Protection Integration Component (SEPIC) does not support automatic upgrade from SEPIC 7.0. You must manually migrate the database and the installation packages of SEPIC 7.0 to SEPIC 7.1 and then upgrade to the latest version. The database and the installation packages are created during the Migration job or during execution of the Install SEP task in SEPIC 7.0.

The SEPIC 7.1 database must have the same collation as is for the SEPIC 7.0 database. Back up the database in SEPIC 7.0. Restore this database in SEPIC 7.1 with a new name. Ensure that while installing Symantec Management Platform 7.1, you specify the new database in the Database Configuration panel of the Symantec Installation Manager.

Note: In this guide, the information that applies to version 7.1 of the product also applies to later releases of the product unless specified otherwise.

See "Migrating from Symantec Management Platform 7.0" on page 28.

See "Migrating Endpoint Protection Integration Component 7.0" on page 128.

Migrating Endpoint Protection Integration Component 7.0

You must migrate the installation packages from Endpoint Protection Integration Component 7.0 to 7.1 and then upgrade to the latest version.

Note: In this guide, the information that applies to version 7.1 of the product also applies to later releases of the product unless specified otherwise.

To migrate the installation packages from Endpoint Protection Integration Component 7.0 to 7.1

1 On the Endpoint Protection Integration Component 7.0 computer, copy all the packages from the following location:

Package type	Location
32-bit packages	<InstallDir>\NSCap\bin\Win32\X86\Symantec Endpoint Protection\Install Package
64-bit packages	<InstallDir>\NSCap\bin\Win32\X86\Symantec Endpoint Protection\Install Package

2 On the Endpoint Protection Integration Component 7.1 computer, copy the packages at the following location:

Package type	Location
32-bit packages	<InstallDir>\NSCap\bin\Win32\X86\Symantec Endpoint Protection\Install Package
64-bit packages	<InstallDir>\NSCap\bin\Win64\X64\Symantec Endpoint Protection\Install Package

After you migrate to Endpoint Protection Integration Component 7.1, you can upgrade to the latest version of the solution.

For details about upgrade, refer to *Symantec™ Endpoint Protection Integration Component Release Notes* of the current release.

See “About migrating Symantec Endpoint Protection Integration Component” on page 127.

Chapter 20

Migrating IT Analytics Solution

This chapter includes the following topics:

About migrating IT Analytics data

IT Analytics Solution was introduced in IT Management Suite 7.1 and therefore its data cannot be migrated from an earlier version of ITMS.

To upgrade IT Analytics Solution and the associated packs you use Symantec Installation Manager.

For more information, see topics on installing the Symantec Management Platform and IT Management Suite solutions in the *IT Management Suite Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/doc5670.

Index

E

H

I

K

M

N

P

R

S

U

V